Свидетелем простоты числа n ($n-1=2^s(2m+1)$) называется такое a из $\{2,3,\dots,n-2\}$*, что*

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

Утверждается, что у чисел вида $5p$ не больше 4 свидетелей простоты.

$5p-1=2^s(2m+1)$

Пусть есть свидетель простоты – a

Тогда верна следующая совокупность

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

(1) Если верно первое условие

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

$$\begin{cases} a^{2m+1} \equiv 1\ (mod\ 5p) \\ a^{p-1} \equiv 1\ (mod\ p)\ (\text{МТФ}) \to a^{\text{НОД}(2m+1,\ p-1)} \equiv 1(mod\ p), a^{\text{НОД}(2m+1,\ 4)} \\ a^4 \equiv 1\ (mod\ 5)\ (\text{МТФ}) \end{cases}$$

$$\equiv 1(mod\ 5)$$

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

i = min(s, $deg_2(p-1)$), то есть мы домножили один из аргументов НОДа на степень двойки, значит значение НОДа изменилось на какую-то степень двойки i, при том что $\text{НОД}(2m+1, p-1)$ не делится на 2.

$$(=)\frac{\text{НОД}(5p-5(p-1)-1, p-1)}{2^i} = \frac{\text{НОД}(4, p-1)}{2^i} = 1$$

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

$a \equiv 1(mod\ p), a \equiv 1(mod\ 5) \to a \equiv 1(mod\ 5p) => a$

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

Т.о. случай (1) невозможен.

(2) Если верно второе условие

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

Для p возможны 2 варианта остатков на 4 (1 и 3). Рассмотрим каждый по отдельности.

1. $p = 4k + 3$

$$a^{2^t(2m+1)} \equiv -1(mod\ p), \left(\frac{-1}{4k+3}\right) = -1 \to t = 0$$

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

$$\begin{cases} a^{2(2m+1)} \equiv 1(mod\ 5p) \\ a^{p-1} \equiv 1\ (mod\ p)\ (\text{МТФ}) \\ a^4 \equiv 1\ (mod\ 5)\ (\text{МТФ}) \end{cases} \to a^{\text{НОД}(2(2m+1),\ p-1)}$$

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

$$\text{НОД}(2(2m+1),\ p-1) = 2$$

$$\text{НОД}(2(2m+1),\ 4) = 2$$

$$\begin{cases} a^2 \equiv 1(mod\ 5p) \\ a^{(2m+1)} \equiv -1\ (mod\ 5p) \end{cases}$$

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

2. $p = 4k + 1$

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

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

$$\begin{cases} a^{20k+4} \equiv 1(mod\ 5p) \\ \begin{cases} a^{4k} \equiv 1(mod\ p)\ (\text{МТФ}) \\ a^4 \equiv 1(mod\ 5)\ (\text{МТФ}) \end{cases} \to a^{4k} \equiv 1\ (mod\ 5p) \end{cases} \to a^4 \equiv 1\ (mod\ 5p)$$

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.

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

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

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

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

- *Решение* $a \equiv 1\ (mod\ p)$ *не подходит, т.к.* $a^{2^t(2m+1)} \equiv -1(mod\ 5p)$
- *При* $a \equiv -1\ (mod\ p)$, $a^{2^t(2m+1)} \equiv -1(mod\ 5p)$ *верно только при* $t = 0$. *Тогда* $a^{(2m+1)} \equiv -1(mod\ 5p)$

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

  $$\begin{cases} a^{2(2m+1)} \equiv 1(mod\ 5p) \\ a^{p-1} \equiv 1\ (mod\ p)\ (\text{МТФ}) \rightarrow a^{\text{НОД}(2(2m+1),\ p-1)} \\ a^4 \equiv 1\ (mod\ 5)\ (\text{МТФ}) \end{cases}$$

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

  $\text{НОД}(2(2m+1),\ p-1) = 2$

  $\text{НОД}(2(2m+1),\ 4) = 2$

  $$\begin{cases} a^2 \equiv 1(mod\ 5p) \\ a^{(2m+1)} \equiv -1\ (mod\ 5p) \end{cases}$$

  $a^{(2m+1)} = (a^2)^m \times a \equiv a$

  $\equiv -1(mod\ n)$

  $-$ противоречие $(a \in \{2, 3, \dots, 5p-2\})$
- *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 a не может быть сравнима с 0 и ± 1 *по модулю 5.*

$a^{2^t(2m+1)} \equiv -1(mod\ 5)$ – *отсюда очевидно, что a не может быть сравнимо с 0 и 1 по модулю 5, если a сравнимо с -1,* *тогда t=0* => $a^{(2m+1)} \equiv -1(mod\ 5p) \rightarrow\ a^{2(2m+1)} \equiv 1(mod\ 5p)$ и $a^4 \equiv 1\ (mod\ 5p) => a^{\text{НОД}(2(2m+1),\ 4)} \equiv 1(mod\ 5p) \rightarrow a^2 \equiv 1(mod\ 5p) \rightarrow a^{(2m+1)} \equiv a(mod\ 5p) \equiv -1(mod\ 5p)\ \rightarrow a = 5p - 1$ – противоречие.

Числа p, 2p, 3p, 4p, 5p имеют разные остатки при делении на 5, тогда числа $r;\ p \pm r;\ 2p \pm r;\ 3p \pm r;\ 4p \pm r;\ 5p - r$ *сравнимы с* $\pm r,\ 1 \pm r, 2 \pm r, 3 \pm r, 4 \pm r$ *т.к. в группе из 5 чисел* $r,\ 1 + r, 2 + r, 3 + r, 4 + r$ *5 различных остатков при делении на 5 и в группе* $-r,\ 1 - r, 2 - r, 3 - r, 4 - r$ *тоже 5 различных остатков, то в данном наборе из 10 чисел каждый остаток при делении на 5 присутствует ровно 2 раза. Тогда, из предложенных 10 вариантов для a найдутся 2 сравнимых с 1, 2 сравнимых с -1 и 2 сравнимых с 0 по модулю 5, а такие нам не подходят. Т.о. вариантов для a остается не больше 4.*

Ч.т.д.