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

$$\begin{bmatrix} a^{2m+1} \equiv 1\ (mod\ n) \\ \exists\ t<s: a^{2^t(2m+1)} \equiv -1 (mod\ n) \end{bmatrix}$$

Теорема

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

Теорема вытекает из Лемм 0 – 4.

Лемма 0

У числа 25 не больше двух свидетелей простоты.

Доказательство:

Все сравнения в доказательстве Леммы 0 по модулю 25, кроме тех, модуль которых подписан.

Наибольший нечетный делитель числа 24 равен 3, степень вхождения двойки в 24 равна 3.

$\varphi(25)=20$. По теореме Эйлера $a^{20}\equiv 1$.

Предположим, есть свидетель простоты a. Тогда возможны 4 случая.

Первый случай: $a^3\equiv 1$.

Из $a^3\equiv 1$ и $a^{20}\equiv 1$ вытекает, что $a^{\text{НОД}(20,\ 3)}\equiv 1 => a\equiv 1$ – противоречие, т.к. $a\in\{2,3,\dots,23\}$.

Второй случай: $a^3\equiv -1$.

Имеем, $a^2=(-1)^6\times a^2\equiv (a^3)^6\times a^2=a^{20}\equiv 1$.

Из $a^3\equiv -1$ и $a^2\equiv 1$ следует, что $a\equiv -1$ – противоречие, т.к. $a\in\{2,3,\dots,23\}$.

Третий случай: $a^6 \equiv -1$.

Имеем, $a^2 = -(-1)^3 \times a^2 \equiv -(a^6)^3 \times a^2 = -a^{20} \equiv -1 => a \equiv \pm 2\ (mod\ 5) => a \in \{3,\ 7,\ 8,\ 12,\ 13,\ 17,\ 18,\ 22\}$. Проверим каждое из этих чисел $3^2 \equiv 22^2 \equiv 9,\ 7^2 \equiv 18^2 \equiv -1,\ 8^2 \equiv 17^2 \equiv 14,\ 12^2 \equiv 13^2 \equiv 19$. Никакие решения, кроме а = 7 и а = 18, не подходят.

Четвертый случай $a^{12} \equiv -1$.

Имеем, $a^{12} \equiv -1 => a^{24} \equiv 1$.

Имеем, $a^{24} \equiv 1$ и $a^{20} \equiv 1 => a^4 \equiv 1$.

Найдем такие а перебором.

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

Никакие решения, кроме а = 7 и а = 18, не подходят.

Таким образом, у числа 25 не больше двух свидетелей простоты.

Лемма доказана

<u>Лемма 1</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 числа 5p – 1.*

Доказательство:

Обозначим через 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 $a^{p-1} \equiv 1\ (mod\ p)$.

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

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

Заметим, что $\text{НОД}\left(\frac{5p-1}{2^s}, p-1\right)$ является нечетным, т.к. один из его аргументов нечетный.

Обозначим через i $\min(\text{s; степень вхождения двойки в } p-1)$. Тогда $\text{НОД}\left(\frac{5p-1}{2^s}, p-1\right) = \frac{\text{НОД}(5p-1,\ p-1)}{2^i}$.

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

$\text{НОД}(4,\ p-1)$ является степенью двойки, при этом $\frac{\text{НОД}(4,\ p-1)}{2^i}$ равно нечетному числу – $\text{НОД}\left(\frac{5p-1}{2^s}, p-1\right)$, следовательно, $\frac{\text{НОД}(4,\ p-1)}{2^i} = 1$.

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

$\text{НОД}(2m+1,\ 4) = 1$, т.к. это НОД нечетного числа и степени двойки.

Из $a \equiv 1(mod\ p)$ и $a \equiv 1(mod\ 5)$ следует, что $a \equiv 1(mod\ 5p)$ – противоречие, т. к. $a \in \{2, 3, \dots, 5p-2\}$.

Лемма доказана

<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 числа 5p – 1.

Доказательство:

Предположим обратное:

Нашлись такие a и p, что $a^{2m+1} \equiv -1(mod\ 5p)$. Из этого следует, что $a^{2(2m+1)} \equiv 1(mod\ 5p)$.

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

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

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

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

Имеем, $\text{НОД}(2(2m+1),\ 4) = 2\text{НОД}(2m+1,\ 4) = 2$.

Из $a^2 \equiv 1\ (mod\ 5)$ и $a^2 \equiv 1\ (mod\ p)$ следует, что $a^2 \equiv 1\ (mod\ 5p)$.

Имеем,

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

Лемма доказана

<u>Лемма 3</u>

Для любого числа вида 5p, где p – простое, которое имеет остаток 3 от деления на 4, не существует такого $a \in \{2, 3, \dots, 5p-2\}$ *и такого* $t < s$, *где s – степень вхождения двойки в 5p – 1, что* $a^{2^t(2m+1)} \equiv -1(mod\ 5p)$, *где* $(2m+1)$ *– наибольший нечетный делитель 5p – 1.*

Доказательство:

Предположим противное:

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

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

$a^{(2m+1)} \equiv -1(mod\ 5p)$, что противоречит Лемме 2.

Лемма доказана

<u>Лемма 4</u>

Для любого числа вида 5p, где $p \neq 5$ *и p – простое, которое имеет остаток 1 от деления на 4, существует не больше 4 таких a из* $\{2, 3, \dots, 5p-2\}$, *для каждого из которых существует такое* $t < s$, *где s – степень*

вхождения двойки в 5p-1, что $a^{2^t(2m+1)} \equiv -1(mod\ 5p)$*, где* $(2m+1)$ *– наибольший нечетный делитель 5p – 1.*

Доказательство:

Пусть существует такое a, что $a^{2^t(2m+1)} \equiv -1(mod\ 5p)$.

Т.к. p сравнимо с 1 по модулю 4, можем представить p в следующем виде: $p = 4k + 1$.

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

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

Имеем, $a^{20k+4} \equiv 1(mod\ 5p)$.

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

Из $a^{20k+4} \equiv 1(mod\ p)$ и $a^{4k} \equiv 1(mod\ p)$ следует, что $a^4 \equiv 1(mod\ p)$.

Из $a^4 \equiv 1(mod\ p)$ и $a^4 \equiv 1(mod\ 5)$ следует, что $a^4 \equiv 1(mod\ 5p)$.

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

Имеем, $a \equiv -1\ (mod\ p)$ и $a^{2^t(2m+1)} \equiv -1(mod\ 5p)$. Это верно только при $t = 0$. Тогда $a^{(2m+1)} \equiv -1(mod\ 5p)$, что противоречит Лемме 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.

Имеем, $a^{2^t(2m+1)} \equiv -1(mod\ 5) -$ отсюда очевидно, что а не может быть сравнимо с 0 и 1 по модулю 5. Если а сравнимо с -1, тогда *t=0* => $a^{(2m+1)} \equiv -1(mod\ 5p)$, что противоречит Лемме 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. Таким образом, вариантов для а остается не больше 4.

Лемма доказана