Ро-метод Полларда.

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$$

$$\mathbb{Z}_n^+ = \{1, 2, \dots, n-1\}$$

$$\mathbb{Z}_n^* = \{z \in \mathbb{Z}_n^+ \,:\, gcd(z, n) = 1\}$$

Заметим, что для каждого числа количество чисел, не взаимно простых с составным n, хотя бы $O(\sqrt{n})$. Тогда можно было бы выбрать много случайных чисел и проверить, что $gcd(z, n) > 1$. Для каждого такого числа вероятность найти делитель будет $\frac{\sqrt{n}}{n} = \frac{1}{\sqrt{n}}$. Нам не хватает такой точности.

Построим функциональный граф для какой-то псевдослучайной функции g (чаще всего $g(x) = x^2+1$ по модулю n) на остатках. Также навесим дополнительное требование на g, чтобы она сохранила остатки (то есть $g(x) \ mod \ a = g(x \ mod \ a) \ mod \ a$, наша функция этому удовлетворяет). Заметим, что в нем произвольный бесконечный путь будет выглядеть как буква ρ — сначала какой-то период, а потом цикл. С учетом случайности функции и парадокса дней рождения в этой букве ρ будет $\sqrt{n}$ вершин.

Пока что мы еще ничего не выиграли, но осталось совсем немного. Возьмем и мысленно сделаем функциональные графы по всем остаткам меньше n (назовем их a). При этом мы явно будем генерировать только путь в функциональном графе для числа n. Поскольку у составного n был делитель меньше, чем $2\sqrt{n}$, то в каком-то функциональном графе мы зациклимся за $O(\sqrt[4]{n})$ шагов. Если мы возьмем все пары (x_i, x_{2i}), то тогда они за линейное время относительно размера буквы ρ будут указывать на одинаковую вершину. А это будет значить, что $|x_i - x_{2i}| \equiv 0 \pmod{a}$. Тогда если a было делителем n, то $gcd(|x_i - x_{2i}|, n) > 1$. Тогда мы нашли какой-то делитель и можно раскладывать рекурсивно.

Алгоритм Миллера-Рабина. Создадим тест-проверку на $a^{n-1} \equiv 1 \pmod{n}$. Если это было верно для всех a от 1 до $n-1$, то число n было простым, потому что тогда оно было взаимно простым со всеми $a < n$. Мы хотим брать случайные числа a, при этом сделать немного итераций. Это называется тестом Ферма.

Просто брать случайные a нельзя — есть числа Кармайкла, которые работают в качестве контртеста. Их какое-то полиномиальное количество, хоть и не очень много.

Сделаем новый тест: $a^2 \equiv 1 \pmod{n}, a \neq 1, a \neq -1$, таких чисел не бывает для простых n (потому что это будет означать что $(a-1)(a+1) \equiv 0 \pmod{n}$)

Рассмотрим $n - 1 = 2^s \cdot k, k \equiv 1 \pmod{2}$.

Сделаем $A(x) = \{x^k, x^{2k}, x^{4k}, \dots, x^{n-1}\}$. Тогда если у нас есть пара соседей $(d, 1), d \neq 1, d \neq -1$, то тогда наш второй тест провалился — n не простое. Если последним элементом последовательности было число $d \neq 1$, то провалился тест Ферма — число составное. Назовем свидетелями такие x, для которых один из этих тестов выполнился, остальных назовем лжецами. Мы хотим показать, что при случайном выборе x-ов, вероятность получить лжеца будет не выше $\frac{1}{2}$.

Тогда $x \in \mathbb{Z}_n^+$, $\mathbb{Z}_n^+ = W \cup L$. А еще запомним, что $\mathbb{Z}_n^*$ — группа.

Пусть наше число не было числом Кармайкла. Тогда $\exists x \in \mathbb{Z}_n^* \,:\, x^{n-1} \not\equiv 1 \pmod{n}$. Тогда можно взять подгруппу $B = \{z \in \mathbb{Z}_n^* : z^{n-1} \equiv 1\}$ (она содержит единицу,)

План: Хотим показать, что $L \subseteq B \subseteq \mathbb{Z}_n^*$

Автор сломался понять доказательство, возможно затехает его позже.