

5.1.2. Тест Соловэя–Штрассена

В основе этого теста лежит следующая теорема.

Теорема 5.3 (критерий Эйлера). Нечетное число n является простым тогда и только тогда, когда для любого целого числа a , $1 \leq a \leq n - 1$, взаимно простого с n , выполняется сравнение

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n} \right) (\text{mod } n). \quad (5.2)$$

Доказательство. Если число n простое, то сравнение (5.2) — это свойство 3 символа Лежандра. Пусть теперь сравнение выполнено, и число n составное. Тогда

$$a^{n-1} = \left(a^{\frac{n-1}{2}} \right)^2 \equiv \left(\frac{a}{n} \right)^2 = 1 (\text{mod } n).$$

Таким образом, для любого числа a , удовлетворяющего условиям теоремы, выполняется сравнение (5.1), и n является числом Кармайкла. Согласно свойству 2 из теоремы 5.2, каноническое разложение числа n имеет вид $n = p_1 p_2 \dots p_s$ (все числа p_i различны). Пусть b — квадратичный невычет по модулю p_1 , то есть $\left(\frac{b}{p_1} \right) = -1$. По китайской теореме об остатках найдем такое число a , что

$$a \equiv b \pmod{p_1}, a \equiv 1 \pmod{p_2}, \dots, a \equiv 1 \pmod{p_s}. \quad (5.3)$$

Вычислим символ Якоби:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right) = \left(\frac{b}{p_1}\right)\left(\frac{1}{p_2}\right)\cdots\left(\frac{1}{p_s}\right) = \left(\frac{b}{p_1}\right) = -1.$$

Подставляя это значение в сравнение (5.2), получаем, что $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, а значит, $a^{\frac{n-1}{2}} \equiv -1 \pmod{p_i}$ для всех i , $1 \leq i \leq s$, что противоречит условию (5.3). \square

Критерий Эйлера лежит в основе следующего вероятностного теста простоты [10].

Алгоритм 5.3. Тест Соловэя–Штрассена.

Вход. Нечетное целое число $n \geq 5$.

Выход. «Число n , вероятно, простое» или «Число n составное».

1. Выбрать случайное целое число a , $2 \leq a \leq n - 2$.
2. Вычислить $r \leftarrow a^{\frac{n-1}{2}} \pmod{n}$.
3. При $r \neq 1$ и $r \neq n - 1$ результат: «Число n составное».
4. Вычислить символ Якоби $s \leftarrow \left(\frac{a}{n}\right)$.
5. При $r \equiv s \pmod{n}$ результат: «Число n составное». В противном случае результат: «Число n , вероятно, простое». \square

На шаге 1 мы снова не рассматриваем числа 1 и $n - 1$, поскольку в силу свойства 3 символа Лежандра сравнение (5.2) для этих чисел выполняется при любом нечетном n . Если $d = \text{НОД}(a, n) > 1$, то d делит и число r , вычисляемое на шаге 2. Таким образом, при проверке неравенства $r \neq 1$ на шаге 3 автоматически проверяется условие $\text{НОД}(a, n) \neq 1$.

Сложность теста Соловэя–Штрассена определяется сложностью вычисления символа Якоби и равна $O(\log^3 n)$.

Определение 5.3. Пусть число n нечетное составное и число a произвольное целое, взаимно простое с n , $2 \leq a \leq n - 1$. Число n называется эйлеровым псевдопростым по основанию a , если выполняется сравнение (5.2), то есть если для числа n алгоритм 5.3 выдает результат «Число n , вероятно, простое».

Теорема 5.3 показывает, что для теста Соловэя–Штрассена не существует чисел, подобных числам Кармайкла, то есть составных чисел, которые были бы эйлеровыми псевдопростыми по всем основаниям a . Этот результат был независимо получен Д. Лемером (D. Lehmer) в 1976 году и Р. Соловэем (R. Solovay), Ф. Штрассеном в 1977 году.

Пример 5.8. Число $n = 527 = 17 \cdot 31$ является эйлеровым псевдопростым по основаниям 1 и 526, поскольку $1^{263} \equiv 526^{263} \equiv 1 \pmod{527}$

$$\text{и } \left(\frac{1}{527} \right) = \left(\frac{526}{527} \right) = 1.$$

□

Пример 5.9. Число $n = 629 = 17 \cdot 37$ является эйлеровым псевдопростым по основаниям 1, 186, 191, 302, 327, 438, 443, 628, поскольку

$$1^{314} \equiv 186^{314} \equiv 443^{314} \equiv 628^{314} \equiv 1 \pmod{629},$$

$$\left(\frac{1}{629} \right) = \left(\frac{186}{629} \right) = \left(\frac{443}{629} \right) = \left(\frac{628}{629} \right) = 1$$

и

$$191^{314} \equiv 302^{314} \equiv 327^{314} \equiv 438^{314} \equiv 628 \pmod{629},$$

$$\left(\frac{191}{629} \right) = \left(\frac{302}{629} \right) = \left(\frac{327}{629} \right) = \left(\frac{438}{629} \right) = -1.$$

□

Пример 5.10. В интервале от 8 до 10000 эйлеровыми псевдопростыми по основанию 7 являются числа 25, 325, 703, 2101, 2353, 2465, 3277, 4525. □

Пример 5.11. Для числа $n = 561$ тест Ферма выдает результат «Число n , вероятно, простое» для всех $320 = \phi(561)$ оснований a . Тест

Соловэя–Штрассена для этого числа выдает такой же результат лишь

для $80 = \frac{\varphi(561)}{4}$ оснований a . Например, при $a = 5$ получаем

$a^{\frac{n-1}{2}} = 5^{\frac{280}{2}} = 5^{280} \equiv 67 \pmod{n}$ и результат «Число n составное» на шаге 3; при

$a = 13$ получаем $a^{\frac{n-1}{2}} = 13^{\frac{280}{2}} = 13^{280} \equiv 1 \pmod{n}$, но $\left(\frac{13}{561}\right) = -1$ и результат «Число n составное» на шаге 5. \square

Теорема 5.4. Для нечетного составного числа n справедливы следующие утверждения.

1. Если число n эйлерово псевдопростое по основанию a и не является таковым по основанию b , то оно не эйлерово псевдопростое по основанию $ab \pmod{n}$.

2. Если число n эйлерово псевдопростое по основаниям a и b , то n псевдопростое по основаниям $ab \pmod{n}$, $ab^{-1} \pmod{n}$ и $a^{-1}b \pmod{n}$.

3. Если число n не является эйлеровым псевдопростым хотя бы по одному основанию a , то n является эйлеровым псевдопростым не более чем по $\frac{\varphi(n)}{2}$ основаниям, где φ — функция Эйлера.

4. Если число n является эйлеровым псевдопростым по основанию a , то оно является и псевдопростым по основанию a .

Доказательство. Первое утверждение докажем от противного. Пусть сравнение (5.2) выполнено для a и для ab и не выполнено для b .

Обозначим $l_a = \left(\frac{a}{n}\right)$. Тогда

$$\begin{aligned} (ab)^{\frac{n-1}{2}} - l_{ab} &= a^{\frac{n-1}{2}} b^{\frac{n-1}{2}} - l_a l_b = a^{\frac{n-1}{2}} b^{\frac{n-1}{2}} - a^{\frac{n-1}{2}} l_b + a^{\frac{n-1}{2}} l_b - l_a l_b = \\ &= a^{\frac{n-1}{2}} (b^{\frac{n-1}{2}} - l_b) + (a^{\frac{n-1}{2}} - l_a) l_b. \end{aligned}$$

Разность $(ab)^{\frac{n-1}{2}} - l_{ab}$ делится на n по предположению, разность $a^{\frac{n-1}{2}} - l_a$ делится на n по условию теоремы, тогда и число $a^{\frac{n-1}{2}}(b^{\frac{n-1}{2}} - l_b)$ должно делиться на n . Но a взаимно просто с n , и разность в скобках не делится на n . Противоречие.

Утверждения 2 и 3 доказываются аналогично утверждениям 2 и 3 теоремы 5.1.

Для доказательства четвертого утверждения возводим в квадрат обе части сравнения (5.2) и получаем сравнение (5.1). \square

Вероятность того, что тест Соловэя–Штассена объявит нечетное составное число n простым, меньше, чем $\frac{1}{2^t}$.

5.1.3. Тест Миллера–Рабина

На сегодняшний день для проверки чисел на простоту чаще всего используется тест Миллера–Рабина, основанный на следующем наблюдении. Пусть число n нечетное и $n - 1 = 2^s r$, где r — нечетное. Если n простое, то для любого $a \geq 2$, взаимно простого с n , выполняется условие (5.1). Разложим число a^{n-1} на множители:

$$\begin{aligned} a^{n-1} - 1 &= a^{2^s r} - 1 = (a^{2^{s-1}r} - 1)(a^{2^{s-1}r} + 1) = \\ &= (a^{2^{s-2}r} - 1)(a^{2^{s-2}r} + 1)(a^{2^{s-1}r} + 1) = \dots = \\ &= (a^{2r} - 1)(a^{2r} + 1) \dots (a^{2^{s-2}r} + 1)(a^{2^{s-1}r} + 1) = \\ &= (a^r - 1)(a^r + 1)(a^{2r} + 1) \dots (a^{2^{s-2}r} + 1)(a^{2^{s-1}r} + 1). \end{aligned}$$

Тогда в последнем произведении хотя бы одна из скобок делится на n , то есть либо $a^r \equiv 1 \pmod{n}$, либо среди чисел $a^r, a^{2r}, \dots, a^{2^{s-1}r}$ найдется сравнимое с -1 по модулю n .

Пример 5.15. Покажем, что число Кармайкла $2465 = 5 \cdot 17 \cdot 29$ не является сильно псевдопростым по основанию 3. Находим представление $2465 - 1 = 2^5 \cdot 77$, то есть $s = 5$, $r = 77$. Рассмотрим значения 2^{2j} для $j = 0, 1, \dots, 5$ по модулю каждого из делителей числа 2465:

	mod 5	mod 17	mod 29	mod 2465
3^{77}	3	12	17	2018
$(3^{77})^2$	-1	8	-1	144
$(3^{77})^{2^2}$	1	13	1	1016
$(3^{77})^{2^3}$	1	-1	1	1886
$(3^{77})^{2^4}$	1	1	1	1
$(3^{77})^{2^5}$	1	1	1	1

В последнем столбце значение -1 можем получить только в том случае, если все вычеты в соответствующей строке равны -1 . Поскольку значения вычетов по разным модулям не зависят друг от друга, вероятность получить -1 по всем модулям достаточно мала. \square

Вероятность того, что тест Миллера–Рабина объявит нечетное составное число n , не являющееся степенью простого числа, простым, меньше, чем $\frac{1}{4}$. Для большинства нечетных составных чисел n оснований, по которым n является сильно псевдопростым, на самом деле гораздо меньше, чем $\frac{\varphi(n)}{4}$.

Пример 5.16. Для составных чисел n вида $(2p + 1)(4p + 1)$, где $2p + 1$, $4p + 1$ — простые числа, p — положительное нечетное, и чисел Кармайкла, состоящих из трех сомножителей, оснований, по которым n является сильно псевдопростым, ровно $\frac{\varphi(n)}{4}$ [8, 11].

Например, для $n = 88831 = 211 \cdot 421$ существует 22050 чисел a , $1 \leq a < n$, взаимно простых с n , для которых выполняется сравнение $a^r \equiv \pm 1 \pmod{n}$, где $r = 44415 = \frac{n-1}{2}$, при этом $\phi(n) = 210 \cdot 420 = 88200 = 4 \cdot 22050$. \square

Замечание. Если число n является сильно псевдопростым по основаниям a и b , то, как правило, n будет сильно псевдопростым и по основанию $ab \pmod{n}$. Поэтому на шаге 2 теста Миллера–Рабина можно выбирать не случайные числа a , а первые несколько простых чисел.

Пусть p_1, p_2, \dots, p_t — первые t простых чисел. Обозначим ψ , наименьшее положительное составное число, которое является псевдопростым по каждому из оснований p_1, p_2, \dots, p_t . Тогда для проверки на простоту произвольного целого числа $n < \psi$, тестом Миллера–Рабина достаточно взять в качестве a первые t простых чисел p_1, p_2, \dots, p_t . В этом случае тест всегда дает верный результат. Например, при $n < 2047$ достаточно выполнить тест для числа $a = 2$; при $n < 1373\,653$ — для чисел 2 и 3; при $n < 25\,326\,001$ — для чисел 2, 3, 5 и т. д.

Лемма 5.5. Пусть для некоторого целого a выполняется сравнение $a^{2^{s-1}r} \equiv -1 \pmod{n}$, где $n-1 = 2^s r$, p — произвольный простой делитель числа n , $p-1 = 2^{s'} r'$, число r' нечетное. Тогда

$$\left(\frac{a}{p} \right) = \begin{cases} -1 & \text{при } s' = s, \\ 1 & \text{при } s' > s. \end{cases}$$

Доказательство [2]. Возведем обе части сравнения $a^{2^{s-1}r} \equiv -1 \pmod{n}$ в нечетную степень r' : $(a^{2^{s-1}r})^{r'} \equiv -1 \pmod{n}$. Это же сравнение справедливо и по модулю любого простого делителя числа n , в том числе и по модулю p . Если предположить, что $s' < s$, то $a^{2^{s'}r'} \not\equiv -1 \pmod{n}$.

Обращение этого свойства и лежит в основе теста Миллера–Рабина.

Алгоритм 5.4. Тест Миллера–Рабина.

Вход. Нечетное целое число $n \geq 5$.

Выход. «Число n , вероятно, простое» или «Число n составное».

1. Представить $n - 1$ в виде $n - 1 = 2^s r$, где число r нечетное.
2. Выбрать случайное целое число a , $2 \leq a \leq n - 2$.
3. Вычислить $y \leftarrow a^r \pmod{n}$.
4. При $y \neq 1$ и $y \neq n - 1$ выполнить следующие действия.
 - 4.1. Положить $j \leftarrow 1$.
 - 4.2. Если $j \leq s - 1$ и $y \neq n - 1$, то
 - 4.2.1. Положить $y \leftarrow y^2 \pmod{n}$.
 - 4.2.2. При $y = 1$ результат: «Число n составное».
 - 4.2.3. Положить $j \leftarrow j + 1$.
 - 4.3. При $y \neq n - 1$ результат: «Число n составное».
5. Результат: «Число n , вероятно, простое». □

В результате выполнения теста для простого числа n в последовательности $a^r \pmod{n}$, $a^{2r} \pmod{n}$, ..., $a^{2^{s-1}r} \pmod{n}$ обязательно перед 1 должна появиться -1 (или, что то же самое, $n - 1 \pmod{n}$). Это означает, что для простого числа n единственными решениями сравнения $y^2 \equiv 1 \pmod{n}$ являются $y \equiv \pm 1 \pmod{n}$. Если число n составное и имеет $k > 1$ различных простых делителей (то есть не является степенью простого числа), то по китайской теореме об остатках существует 2^k решений сравнения $y^2 \equiv 1 \pmod{n}$. Действительно, для любого простого делителя p_i числа n существует два решения указанного сравнения: $y \equiv \pm 1 \pmod{p_i}$. Поэтому k таких сравнений дают 2^k наборов решений по модулям p_i , содержащих элементы ± 1 .

Сложность алгоритма 5.4 равна $O((\log n)^3)$.

Определение 5.4. Пусть число n нечетное простое, $n - 1 = 2^s r$, где r — нечетное, и a — произвольное целое число, $1 \leq a \leq n - 1$, взаимно простое с n . Число n называется *сильно псевдопростым по основанию* a , если $a^r \equiv 1 \pmod{n}$ или если существует такое целое j , $0 \leq j \leq s - 1$, что $a^{2^j r} \equiv -1 \pmod{n}$.

Пример 5.12. Для числа $n = 105 = 3 \cdot 5 \cdot 7$ имеем: $n - 1 = 2^3 \cdot 13$, то есть $s = 3$, $r = 13$. Число 105 является сильно псевдопростым только по основаниям 1 и 104.

Более того, любое целое число n , являющееся произведением первых $k \geq 2$ нечетных чисел, является сильно псевдопростым только по двум основаниям, а именно, 1 и $n - 1$. \square

Пример 5.13. Для числа $n = 629 = 17 \cdot 37$ имеем: $n - 1 = 2^2 \cdot 157$, то есть $s = 2$, $r = 157$, $2r = 314$. Число 629 является сильно псевдопростым по основаниям 1, 191, 302, 327, 438, 628 поскольку

$$1^{157} \equiv 1 \pmod{629}, \quad 628^{157} \equiv -1 \pmod{629},$$

$$191^{314} \equiv 302^{314} \equiv 327^{314} \equiv 438^{314} \equiv -1 \pmod{629}. \quad \square$$

Пример 5.14. В интервале от 8 до 10000 сильно псевдопростыми по основанию 7 являются числа 25, 325, 703, 2101, 2353, 4525:

n	s	r	$7^r \pmod{n}$	$7^{2r} \pmod{n}$
25	3	3	18	-1
325	2	81	307	-1
703	1	351	1	
2101	2	525	-1	
2353	4	147	343	-1
4525	2	1131	343	-1

Пример 5.15. Покажем, что число Кармайкла $2465 = 5 \cdot 17 \cdot 29$ не является сильно псевдопростым по основанию 3. Находим представление $2465 - 1 = 2^5 \cdot 77$, то есть $s = 5$, $r = 77$. Рассмотрим значения 2^{2jr} для $j = 0, 1, \dots, 5$ по модулю каждого из делителей числа 2465:

	mod 5	mod 17	mod 29	mod 2465
3^{77}	3	12	17	2018
$(3^{77})^2$	-1	8	-1	144
$(3^{77})^{2^2}$	1	13	1	1016
$(3^{77})^{2^3}$	1	-1	1	1886
$(3^{77})^{2^4}$	1	1	1	1
$(3^{77})^{2^5}$	1	1	1	1

В последнем столбце значение -1 можем получить только в том случае, если все вычеты в соответствующей строке равны -1 . Поскольку значения вычетов по разным модулям не зависят друг от друга, вероятность получить -1 по всем модулям достаточно мала. \square

Вероятность того, что тест Миллера–Рабина объявит нечетное составное число n , не являющееся степенью простого числа, простым, меньше, чем $\frac{1}{4}$. Для большинства нечетных составных чисел n оснований, по которым n является сильно псевдопростым, на самом деле гораздо меньше, чем $\frac{\phi(n)}{4}$.

Пример 5.16. Для составных чисел n вида $(2p + 1)(4p + 1)$, где $2p + 1$, $4p + 1$ — простые числа, p — положительное нечетное, и чисел Кармайкла, состоящих из трех сомножителей, оснований, по которым n является сильно псевдопростым, ровно $\frac{\phi(n)}{4}$ [8, 11].

Например, для $n = 88831 = 211 \cdot 421$ существует 22050 чисел a , $1 \leq a < n$, взаимно простых с n , для которых выполняется сравнение $a^r \equiv \pm 1 \pmod{n}$, где $r = 44415 = \frac{n-1}{2}$, при этом $\phi(n) = 210 \cdot 420 = 88200 = 4 \cdot 22050$. \square

Замечание. Если число n является сильно псевдопростым по основаниям a и b , то, как правило, n будет сильно псевдопростым и по основанию $ab \pmod{n}$. Поэтому на шаге 2 теста Миллера–Рабина можно выбирать не случайные числа a , а первые несколько простых чисел.

Пусть p_1, p_2, \dots, p_t — первые t простых чисел. Обозначим ψ , наименьшее положительное составное число, которое является псевдопростым по каждому из оснований p_1, p_2, \dots, p_t . Тогда для проверки на простоту произвольного целого числа $n < \psi$, тестом Миллера–Рабина достаточно взять в качестве a первые t простых чисел p_1, p_2, \dots, p_t . В этом случае тест всегда дает верный результат. Например, при $n < 2047$ достаточно выполнить тест для числа $a = 2$; при $n < 1373\,653$ — для чисел 2 и 3; при $n < 25\,326\,001$ — для чисел 2, 3, 5 и т. д.

Лемма 5.5. Пусть для некоторого целого a выполняется сравнение $a^{2^{s-1}r} \equiv -1 \pmod{n}$, где $n-1 = 2^s r$, p — произвольный простой делитель числа n , $p-1 = 2^{s'} r'$, число r' нечетное. Тогда

$$\left(\frac{a}{p} \right) = \begin{cases} -1 & \text{при } s' = s, \\ 1 & \text{при } s' > s. \end{cases}$$

Доказательство [2]. Возведем обе части сравнения $a^{2^{s-1}r} \equiv -1 \pmod{n}$ в нечетную степень r' : $(a^{2^{s-1}r})^{r'} \equiv -1 \pmod{n}$. Это же сравнение справедливо и по модулю любого простого делителя числа n , в том числе и по модулю p . Если предположить, что $s' < s$, то $a^{2^{s'}r'} \not\equiv -1 \pmod{p}$.

может быть сравнимо с 1 по модулю p , а это противоречит малой теореме Ферма. Таким образом, возможен лишь случай $s' \geq s$.

При $s' = s$ получаем

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^r \equiv \left(a^{\frac{p-1}{2}}\right)^r = (a^{2^{s-1}r})^r = (a^{2^{s-1}r})^r \equiv -1 \pmod{p}.$$

При $s' > s$, возводя обе части сравнения $(a^{2^{s-1}r})^r \equiv -1 \pmod{p}$ в степень $2^{s'-s}$, получаем

$$1 \equiv ((a^{2^{s-1}r})^r)^{2^{s'-s}} = (a^{2^{s-1}r})^r = \left(\frac{a}{p}\right)^r = \left(\frac{a}{p}\right) \pmod{p}. \quad \square$$

Лемма 5.6. Пусть для некоторого целого a и некоторого целого j выполняется сравнение $a^{2^{j-1}r} \equiv -1 \pmod{n}$, где $n-1 = 2^s r$, $1 \leq j \leq s-1$, p — произвольный простой делитель числа n , $p-1 = 2^s r'$, число r' нечетное. Тогда

$$\left(\frac{a}{p}\right) = \begin{cases} -1 & \text{при } s' = j, \\ 1 & \text{при } s' > j. \end{cases}$$

Доказательство проводится аналогично предыдущей лемме [2].

Теорема 5.7. Если число n является сильно псевдопростым по основанию a , то оно является эйлеровым псевдопростым по основанию a .

Доказательство [2]. Запишем $n-1$ в виде $n-1 = 2^s r$, где число r нечетное. Рассмотрим три случая.

Случай 1. Пусть $a^r \equiv 1 \pmod{n}$. Тогда $a^{\frac{n-1}{2}} = a^{2^{s-1}r} = (a^r)^{2^{s-1}} \equiv 1 \pmod{n}$. Чтобы выполнялось сравнение (5.2), число a должно быть квадратичным вычетом по модулю n . По свойствам символа Якоби получаем последовательность равенств

$$1 = \left(\frac{1}{n} \right) = \left(\frac{a^r}{n} \right) = \left(\frac{a}{n} \right)^r = \left(\frac{a}{n} \right),$$

поскольку число r нечетное.

Случай 2. Пусть $a^{\frac{n-1}{2}} = a^{2^{s-1}r} \equiv -1 \pmod{n}$. Теперь число a должно быть квадратичным невычетом по модулю n . Разложим число n на простые множители: $n = p_1 p_2 \dots p_m$, где числа p_i не обязательно различны, и представим $p_i - 1 = 2^{s_i} r_i$, где числа r_i нечетные. Пусть k — количество тех чисел p_i , для которых $s_i = s$ (сомножители p_i считаются с учетом кратности). Согласно лемме 5.5, для всех i выполняется неравенство $s_i \geq s$, от-

$$\text{куда } \left(\frac{a}{n} \right) = \prod_i \left(\frac{a}{p_i} \right) = (-1)^k.$$

Кроме того, $p_i = 2^{s_i} r_i + 1 = 2^s r_i + 1 \equiv 2^s + 1 \pmod{2^{s+1}}$ при $s_i = s$, $p_i = 2^{s_i} r_i + 1 \equiv 1 \pmod{2^{s+1}}$ при $s_i > s$ и $n = 2^s r + 1 \equiv 2^s + 1 \pmod{2^{s+1}}$. Тогда

$$2^s + 1 \equiv n = p_1 p_2 \dots p_m \equiv (2^s + 1)^k \equiv k2^s + 1 \pmod{2^{s+1}},$$

откуда $k \equiv 1 \pmod{2}$, то есть число k нечетное и $\left(\frac{a}{n} \right) = (-1)^k = -1$.

Осталось рассмотреть случай, когда $a^{2^{j-1}r} \equiv -1 \pmod{n}$ для некоторого j , $1 \leq j \leq s-1$. Возводя обе части сравнения в нужную степень

двойки, получаем $a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$. Таким образом, для того чтобы число n было эйлеровым псевдопростым, число a должно быть квадратичным

вычетом по модулю n . Так же, как в случае 2, получаем, что $\left(\frac{a}{n} \right) = (-1)^k$.

Воспользовавшись теперь леммой 5.6 и проводя рассуждения, аналогичные предыдущему случаю, получаем $n = 2^s r + 1 \equiv 1 \pmod{2^{j+1}}$ и

$$1 \equiv n = p_1 p_2 \dots p_m \equiv (2^j + 1)^k \equiv k2^j + 1 \pmod{2^{j+1}},$$

откуда $k \equiv 0 \pmod{2}$, то есть число n четное и $\left(\frac{a}{n}\right) = (-1)^k = 1$. □

Таким образом, если число n сильно псевдопростое по основанию a , то n — эйлерово псевдопростое по основанию a . Если число n эйлерово псевдопростое по основанию a , то n — псевдопростое по основанию a (рис. 5.2).

Посмотрим, когда условия эйлеровой и сильной псевдопростоты эквивалентны.

Теорема 5.8. Число $n \equiv 3 \pmod{4}$ является сильно псевдопростым по основанию a тогда и только тогда, когда n является эйлеровым псевдопростым по основанию a .

Доказательство. Пусть число $n = 3 + 4k$, где $k \in \mathbb{Z}$, сильно псевдопростое по основанию a . Запишем $n - 1 = 2 + 4k = 2 \cdot (2k + 1)$, то есть, по определению сильно псевдопростого числа, $s = 1$, $r = 2k + 1$ и $a^{\frac{n-1}{2}} = a^r \equiv \pm 1 \pmod{n}$. Докажем, что число ± 1 в правой части сравнения совпадает с символом Якоби $\left(\frac{a}{n}\right)$. Вычисляем:

$$\left(\frac{1}{n}\right) = 1, \quad \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = (-1)^{2k+1} = -1,$$

то есть $\left(\frac{\pm 1}{n}\right) = \pm 1$. Тогда

$$\left(\frac{a}{n}\right) = \left(\frac{a \cdot (a^{(n-3)/4})^2}{n}\right) = \left(\frac{a^{(n-1)/2}}{n}\right) = \left(\frac{\pm 1}{n}\right) = \pm 1 \equiv a^{\frac{n-1}{2}} \pmod{n},$$

и число n эйлерово псевдопростое по основанию a .

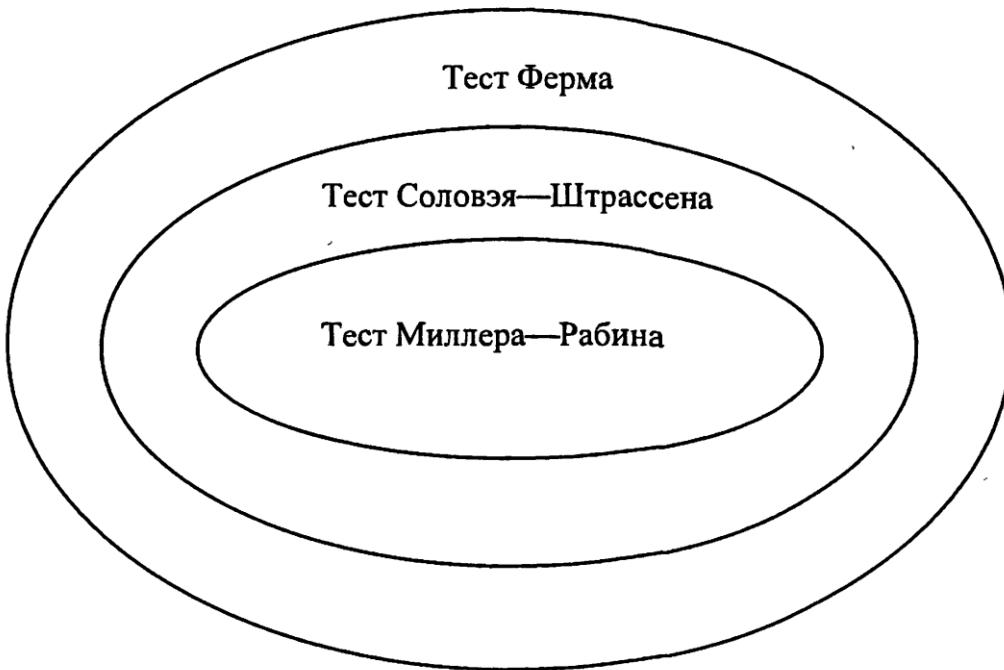


Рис. 5.2. Соотношение между основаниями, по которым данное число n проходит вероятностные тесты проверки на простоту

Обратно, пусть число $n = 3 + 4k$, где $k \in \mathbb{Z}$, эйлерово псевдопростое по основанию a . Для того чтобы n было сильно псевдопростым, должно выполняться либо сравнение $a^r = a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$, либо при $j = 0$ сравнение $a^{2^j r} = a^{2^0 r} = a^r = a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, то есть должно быть $a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$. А для эйлеровых псевдопростых чисел это имеет место по определению. \square