1 Задачи работы

Каждое из указанных чисел проверить на простоту с помощью тестов: Ферма, Соловэя-Штрассена, Рабина-Миллера.

В отчёте привести:

– Результат проверки каждым из тестов для каждого числа - "вероятно простое" или "составное".

– Для составного числа - основание, для которого нарушается условие простоты; показать какое именно условие нарушается.

– Для простого числа - 5 оснований, для которых условие простоты выполняется; показать выполнимость этого условия.

– Для каждого из тестов привести пример двух-трех чисел Кармайкла (не менее 30 десятичных знаков каждое; указать источник) и признаки того, что данное число Кармайкла является "простым" и составным. Привести разложение чисел Кармайкла.

2 Теоретические сведения

2.1 Тест Ферма

Согласно малой теореме Ферма для простого числа произвольного целого числа a, $1 \leq a \leq p - 1$, выполняется сравнение:

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

Следовательно, если для нечетного и существует такое целое a, что $1 \leq a \leq n$, НОД$(\text{a}, n) = 1$ и $a^{n-1}(mod\ n) = 1$, то число n составное. Отсюда получаем следующий вероятностный алгоритм проверки числа на простоту.

Теорема 1:

Для нечетного составного числа $n > 0$ справедливы следующие утверждения:

1. Число и является псевдопростым по основанию a тогда и только тогда, когда $n - 1$ делится на порядок числа a по модулю n.

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

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

2.2 Тест Соловэя-Штрассена

Критерий Эйлера:

Нечетное число n является простым тогда и только тогда, когда для любого целого числа a, $1 \leq \text{a} \leq n-1$, взаимно простого с n, выполняется сравнение: $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)\ (mod\ n)$.

Критерий Эйлера лежит в основе следующего вероятностного теста простоты.

Алгоритм. Тест Соловэя-Штрассена:

Вход: нечетное число n≥5.

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

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

На шаге 1 мы снова не рассматриваем числа 1 и n-1, поскольку в силу свойства символа Лежандра сравнение $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)(mod\ n)$ 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:

Пусть число n нечетное составное и число a проивзольное целое, взаимно простое с n, $2 \leq a \leq n-1$. Число n называется эйлеровым псевдопростым по основанию a, если выполняется сравнение $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)$ (mod n), то есть для числа n тест Соловэя-Штрассена выдает результат: «Число n, вероятно, простое».

Вероятность того, что тест Соловея-Штрассена объявит нечетное составное число n простым, меньше, чем $\frac{1}{2^t}$.

2.3 Тест Рабина-Миллера

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 сравнения

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

Разложим число a^{n-1} на множители:

$a^{n-1}-1=\left(a^{2^{s-1}r}-1\right)\left(a^{2^{s-1}r}+1\right)=(a^{2^{s-2}r}-1)(a^{2^{s-2}r}+1)\left(a^{2^{s-1}r}+1\right)=..=(a^{2r}-1)\ (a^{2r}+1)\ldots\left(a^{2^{s-2}r}+1\right)\left(a^{2^{s-1}r}+1\right)=(d-1)(d+1)(a^{2r}+1)..\left(a^{2^{s-2}r}+1\right)\left(a^{2^{s-1}r}+1\right)=(d-1)$.

Тогда в последнем произведении хотя бы одна из скобок делится на n, то есть либо $d \equiv 1\ (mod\ n)$, либо среди чисел a^{r}, a^{2r},.., $a^{2^{s-1}}$ найдется сравнимое с -1 по модулю n. Обращение этого свойства и лежит в основе теста Рабина-Миллера:

Алгоритм. Тест Рабина-Миллера.

Вход: нечетное 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 r – нечетное.
2. Выбрать случайное целое число a, $2 \leq a \leq n-2$.
3. Вычислить $y \leftarrow a^r (mod\ n)$.
4. При $y \neq 1$ и $y \neq n-1$ выполнить следующие действия.
5. Положить $j \leftarrow 1$.
6. Если $j \leq s-1$ и $y \neq n-1$, то

7. Положить $y \leftarrow y^2 (mod\ n)$.
8. При $y = 1$ результат: «Число n - составное».
9. Положить $j \leftarrow j + 1$.
10. При y $\neq n - 1$ результат: «Число n - составное».
11. Результат: «Число n, вероятно, простое».

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

Определение:

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 $d \equiv 1\ (mod\ n)$, или если существует такое целое j, $0 \leq j \leq s - 1$, что $a^{2^j r} \equiv -1\ (mod\ n)$.

3 Ход работы

3.1 Результаты работы программы

Разработанная программа была запущена для всех чисел. Результаты работы программы представлены в Таблица 1-4.

Таблица 1 – Результаты работы программы для числа: 23839073123744770321

Тест	Результат	Основание a	Какое условие было нарушено (для составных чисел)
Ферма	Вероятно простое	18364835125006112904 11755812382287123854 21921042562405472140 9878312866181274364 17691689151730980976	–
Соловэя-Штрассена	Вероятно простое	10604533931692949133 13264858554679642917 9657188965543725953 14204519862537391890	–

		2274305626733071050 5	
Рабина-Миллера	Вероятно простое	6644743707806233970 1338733891642400194 5 3258945222897464007 1115401954715903691 5 1144875624884543947 3	–

Таблица 2 – Результаты работы программы для числа: 501310093808206482030721454984139339687 7

Тест	Результат	Основание a	Какое условие было нарушено
Ферма	Вероятно простое	45334629456982144196036293439969954678 1 21065973824782997098612194622436032397 6 16503663407585249957696665094831966506 2 13124451089350521896539868949141849406 3 12476580408483032873766931967160041264 30	–
Соловэя-Штрассена	Вероятно простое	17082132891844225757554678568312112739 46 39266677957114609295060505476210522671 4 37701082769886014837574735906882099894 10 39637849320458430438979267001934150483 80 46879343691525194894088941876430955799 52	–
Рабина-Миллера	Вероятно простое	17346553967036150512604500994870416236 1 19487472587754701038536454794111088515 15 18992456768164156931559471608456523849 57 16817836005265447411127094723361215461 45 33773253001468405379253025024220606256 52	–

Таблица 3 – Результаты работы программы для числа: 521160336997010986204649633495982214849

Тест	Результат	Основание a	Какое условие было нарушено
Ферма	Составное	17389097104308147269 0127060537123367912	$r = a^{n-1}(mod\ n) = 1$
Соловэя-Штрассена	Составное	85114170406972282700 645020413374868882	$r = a^{n-1}(mod\ n) = 1$ и $r = a^{n-1}(mod\ n) = n - 1$
Рабина-Миллера	Составное	29742972459988559022 7853286353296193672	$y = n - 1$

Таблица 4 – Результаты работы программы для числа: 43290080466165998487128620582188088198180891483436678106330046919786939765637379

Тест	Результат	Основание a	Какое условие было нарушено
Ферма	Составное	29429773544005401588 57127073693202145259 70343943828369466953 5110761509972774770	$r = a^{n-1}(mod\ n) = 1$
Соловэя-Штрассена	Составное	40681123433648413186 01523101500666587292 82558663072640505656 92681286656895673460	$r = a^{n-1}(mod\ n) = 1$ и $r = a^{n-1}(mod\ n) = n - 1$
Рабина-Миллера	Составное	19538808111606327810 21953799156585658344 70179011038755912103 71766160150067241492	$y = n - 1$

Для тестирования были также найдены числа Кармайкла, имеющие следующие разложения на множители: $n_1 = 32809426840359564991177172754241 = 13 * 17 * 19 * 23 * 29 * 31 * 37 * 41 * 43 * 61 * 67 * 71 * 73 * 97 * 127 * 199 * 281 * 397$ $n_2 = 2810864562635368426005268142616001 = 13 * 17 * 19 * 23 * 29 * 31 * 37 * 41 * 43 * 61 * 67 * 71 * 73 * 109 * 113 * 127 * 151 * 281 * 353$

$n_3 = 349407515342287435050603204719587201 = 13 * 17 * 19 * 23 * 29 * 31 * 37 * 41 * 43 * 61 * 67 * 71 * 73 * 97 * 101 * 109 * 113 * 151 * 181 * 193 * 641$

Результаты работы программы для чисел Кармайкла отражены в Таблица 5-7.

Таблица 5 – Результаты работы программы для числа: 32809426840359564991177172754241

Тест	Результат	Основание a	Какое условие было нарушено
Ферма	Составное	6104268093869046018416905129686	$r = a^{n-1}(mod\ n) = 1$
	Возможно простое	31142082208542686639796981803318	–
	Возможно простое	11132961134469543433054248800733	–
	Возможно простое	20767656219789623872779868482760	–
	Возможно простое	4070173701011662760494583635168	–
Соловэя-Штрассена	Составное	19775369428483152658650074777882	$r = \left(\frac{a}{n}\right)$
	Возможно простое	13693453095802065627119145564582	–

	Составное	25345526818940161393575870320347	$r = a^{n-1} (mod\ n) = 1$ и $r = a^{n-1} (mod\ n) = n - 1$
	Составное	6863491459929458450758705771389	$r = a^{n-1} (mod\ n) = 1$ и $r = a^{n-1} (mod\ n) = n - 1$
	Составное	8137578641243138200081960667653	$r = \left(\frac{a}{n}\right)$
Рабина-Миллера	Составное	15145986866273838193904920324883	$y = n - 1$
	Составное	5703307116880694917158881096342	$y = n - 1$
	Составное	4045582550590324654233985643323	$y = n - 1$
	Составное	19332546895996601093739147766113	$y = n - 1$
	Составное	12279227512344969618313276311534	$y = n - 1$

Таблица 6 – Результаты работы программы для числа: 2810864562635368426005268142616001

Тест	Результат	Основание a	Какое условие было нарушено
Ферма	Возможно простое	1757350456690436355876248083395793	–

	Составное	1220199842992357462557952499040535	$r = a^{n-1}(mod\ n) = 1$
	Составное	253383230309108829655741774530132	$r = a^{n-1}(mod\ n) = 1$
	Возможно простое	187356726231454269062209494149824	–
	Возможно простое	632234476380798674819716220810336	–
Соловэя-Штрассена	Составное	2185817542618962942528922619159289	$r = a^{n-1}(mod\ n) = 1$ и $r = a^{n-1}(mod\ n) = n - 1$
	Составное	1832717533636296317453415030052909	$r = a^{n-1}(mod\ n) = 1$ и $r = a^{n-1}(mod\ n) = n - 1$
	Составное	963330000780276302058486173309356	$r = a^{n-1}(mod\ n) = 1$ и

			$r = a^{n-1}(mod\ n) = n - 1$
	Составное	2357037347451952048449237565664526	$r = \left(\frac{a}{n}\right)$
	Возможно простое	109730550695799760595640909350489	–
Рабина-Миллера	Составное	1816247048574547144025250352026622	$y = n - 1$
	Составное	2306050557959898552480181773415831	$y = n - 1$
	Составное	1696026936644282184693119187007741	$y = n - 1$
	Составное	2572475343851354928289610101727858	$y = n - 1$
	Составное	1571729975788588456948105024885037	$y = n - 1$

Таблица 7 – Результаты работы программы для числа: 349407515342287435050603204719587201

Тест	Результат	Основание a	Какое условие было нарушено
Ферма	Возможно простое	211606452552277933344816614922271425	–
	Возможно простое	68319612888939461762197893717910485	–
	Составное	45642247920876201788343092565170083	$r = a^{n-1}(mod\ n) = 1$
	Возможно простое	235974378878593115039852942975373057	–
	Возможно простое	221490516127953658049502622930672368	–

Соловэя-Штрассена	Составное	93683944333632261417111103246726089	$r = a^{n-1}(mod\ n) = 1$ и $r = a^{n-1}(mod\ n) = n-1$
	Составное	184752343726692137046050524174082870	$r = a^{n-1}(mod\ n) = 1$ и $r = a^{n-1}(mod\ n) = n-1$
	Составное	103195068589328636405977634058709576	$r = a^{n-1}(mod\ n) = 1$ и $r = a^{n-1}(mod\ n) = n-1$
	Составное	130778705772149058336137161450646780	$r = a^{n-1}(mod\ n) = 1$ и $r = a^{n-1}(mod\ n) = n-1$

	Составное	27235865192343305586407743517922065 3	$r = a^{n-1}(mod\ n) = 1$ и $r = a^{n-1}(mod\ n) = n-1$
Рабина-Миллера	Составное	14157045284585595532536853673158530 2	$y = n - 1$
	Составное	23310146110924686752037283668446101 3	$y = n - 1$
	Составное	16778291258253442730537782449653135 1	$y = n - 1$
	Составное	25439700251158291280906712127621621 2	$y = n - 1$
	Составное	22243573623259752741526093627679500	$y = n - 1$

4 Выводы

В ходе выполнения лабораторной работы были реализованы три различных алгоритма для проведения проверки на простоту числа. При запуске программы было показано, что тесты одинаково работают для некоторых случайных чисел, если они не являются числами Кармайкла. Для чисел Кармайкла тест Рабина-Миллера не допустил ошибок, что может говорить о большей надежности этого теста в сравнении с остальными.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1 «THE CARMICHAEL NUMBERS UP TO 10^16» Richard G.E. Pinch (URL: https://arxiv.org/pdf/math/9803082)