Алгоритм Миллера

Подготовил Соломатин Никита

Как отличить составное число от простого

Существует довольно эффективный способ убедиться, что заданное число является составным, не разлагая это число на множители. Согласно малой теореме Ферма, если число *N* простое, то для любого целого *a*, не делящегося на *N*, выполняется сравнение:

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

Если же при каком-то *a* это сравнение нарушается, можно утверждать, что *N* – составное.

Сложность заключается в поиске такого числа *a*.

Числа Кармайкла

Для поиска числа *a* можно попытаться испытывать все целые числа подряд, начиная с 2. Или выбирать случайные числа в промежутке

$$1 < a < N$$

Однако, такой подход не всегда дает нужный результат. Имеются составные числа *N*, обладающие вышеописанным свойством.

Рассмотри число 561. В качестве чисел *a* возьмем любое из следующих: 2, 10 или 16:

т.к. 2|560, 10|560 и 16|560, то с помощью малой теоремы Ферма легко проверить что 561 является простым ($2^{560} \equiv 1\ (mod\ 561)$, $10^{560} \equiv 1\ (mod\ 561)$ и $16^{560} \equiv 1\ (mod\ 561)$).

Однако это число можно разложить:

$$561 = 3 * 11 * 17$$

Вид чисел Кармайкла

Числа Кармайкла имеют вид:

$$N = p_1 * \ldots * p_k,$$

где p_i - простые, различные числа, $k \geq 3$ причем $N - 1$ делится на каждую разность $p_i - 1$.

Недавно была решена проблема о бесконечности множества таких чисел.

Первые 4 числа Кармайкла:

561=3*11*17
1105=5*13*17
1729=7*13*19
2465=5*17*29

Решение Миллера

Если *N* – простое число, $N-1=2^s*t$, где *t* нечетно, то согласно малой теореме Ферма для каждого *a* с условием (a, N) = 1, хотя бы одна из скобок в произведении

$$(a^t-1)*(a^t+1)*(a^{2t}+1)*\ldots*\left(a^{2^{s-1}*t}+1\right)=a^{N-1}-1$$

делится на *N*.

Пусть *N* – нечетное составное число, $N - 1 = 2^s * t$, где *t* нечетно. Назовем целое число *a*, $1 < a < N$, *«хорошим»* для *N*, если нарушается одно из двух условий:

α) N не делится на a

β) $a^t \equiv 1\ (mod\ N)$ или существует целое k, $0 \leq k <$ s, такое, что

$$a^{2^k * t} \equiv 1\ (mod\ N)$$

Алгоритм, доказывающий непростоту числа

1. Выберем случайным образом число *a*, $1 < a < N$, и проверим для этого числа указанные выше свойства:

α) *N* не делится на *a*

β) $a^t \equiv 1 \ (mod\ N)$ или существует целое *k*, $0 \leq k < \mathrm{s}$, что

$$a^{2^k * t} \equiv -1 \ (mod\ N)$$

2. Если хотя бы одно условие нарушается, то *N* составное

3. Если выполнены оба условия, то возвращаемся к шагу 1 и выбираем другое число.

Алгоритм Миллера

Согласно этому алгоритму достаточно проверить условия *α)* и *β)* для всех целых чисел *a*, $2 \leq a \leq f(N)$. Если при каком-нибудь *a* из указанного промежутка нарушается одно из условий *α)* или *β)*, число *N* составное. В противном случае оно будет простым или является степенью простого числа.

Функция f(N)

В 1952 г. Анкени доказал, что для каждого простого числа q существует квадратичный невычет a, удовлетворяющий неравенствам $2 \leq \mathrm{a} \leq c * (\ln q)^2$ при некоторой достаточно большой константе c.

Константа c = 70 была получена позднее, но впоследствии в 1985 г. Эрик Бах уменьшил коэффициент до 2.

Точная формулировка алгоритма Миллера

1. Проверить, выполняется ли равенство $N = m^s$ при некоторых $s, m \in N, s \geq 2$. Если выполняется, то *N* – составное число, и алгоритм останавливается.

2. Выполнить следующие шаги для всех $a \leq f(N)$:

а) Проверить условие a|N

б) Проверить условие $a^{n-1} \not\equiv 1 (\mathrm{mod}\ \mathrm{N})$

в) Выяснить, верно ли, что при некотором *k*, $1 \leq k \leq \nu_2(N-1)$

$$1 < \text{НОД}\left(a^{\frac{N-1}{2^k}} - 1\ (mod\ N), N\right) < N$$

3. Если мы дошли до этого шага, то *N* – простое число.

Пример

1.

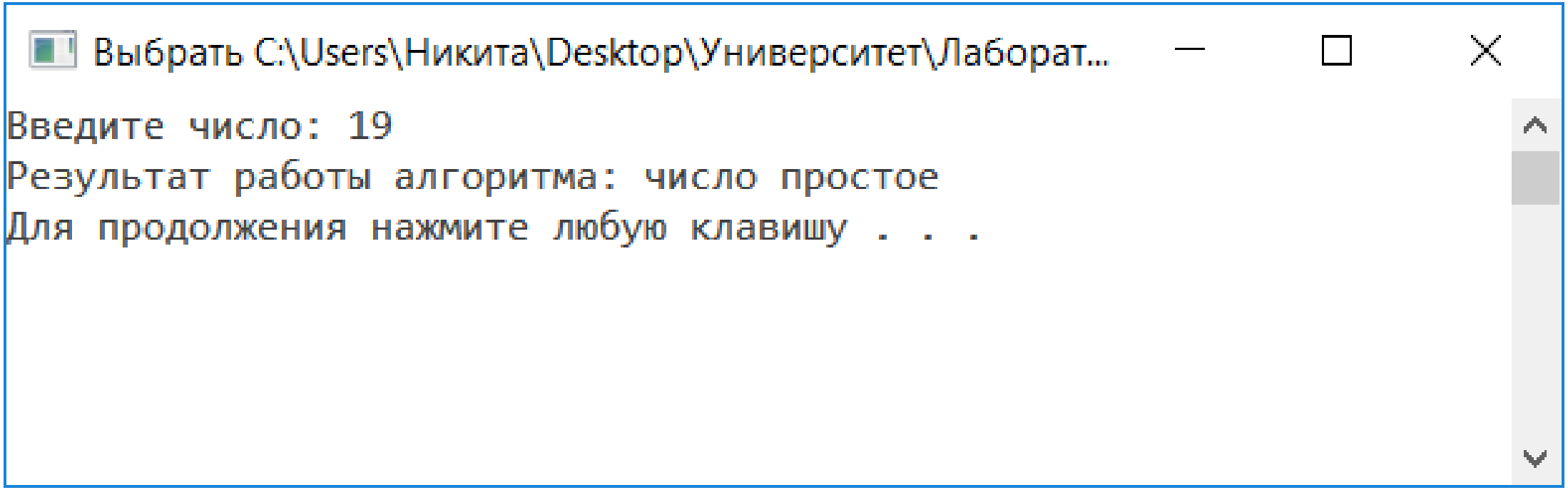
m	2	2	2	2	3	3	4	4	5
s	2	3	4	5	2	3	2	3	2
$p = m^s$	4	8	16	32	9	27	16	64	25

2.

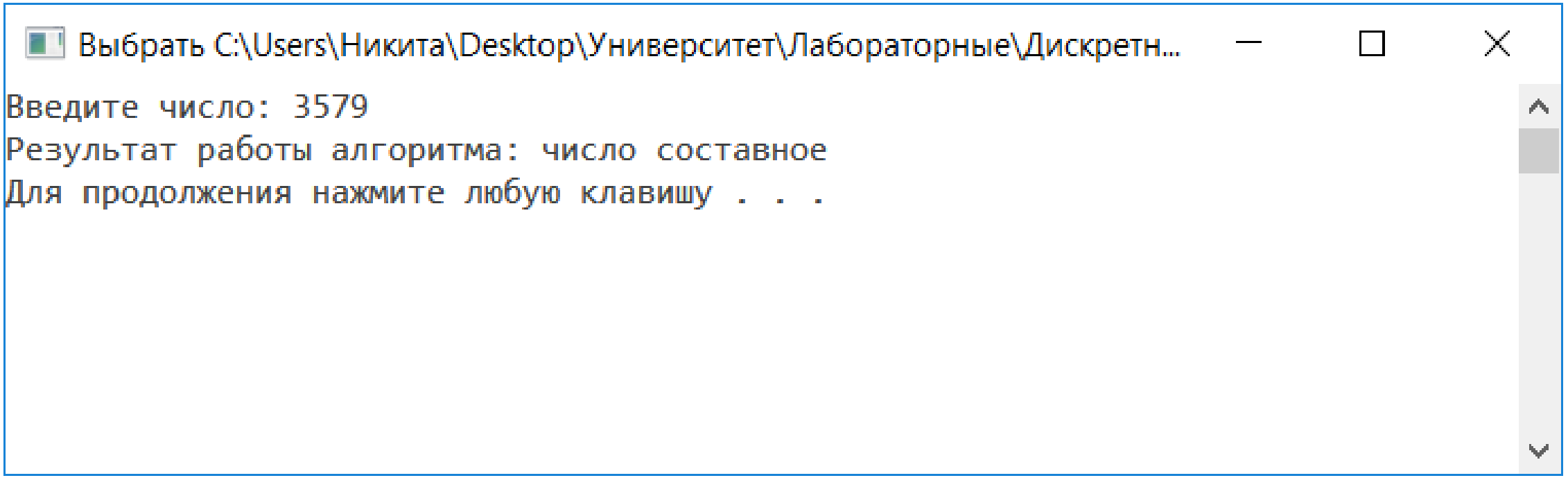
$$f(N)=2 * (\ln 19)^2 = 16$$

$$k = 1$$

a	2	3	5	7	11	13	17
a|N	нет	нет	нет	нет	нет	нет	нет
$a^{N-1} \bmod N$	1	1	1	1	1	1	1
НОД $\left(a^{\frac{N-1}{2^k}} - 1 \ (mod\ N), N\right)$	1						


Выбрать C:\Users\Никита\Desktop\Университет\Лаборат...
Введите число: 19
Результат работы алгоритма: число простое
Для продолжения нажмите любую клавишу . . .

Пример работы программы для числа 3579



Недостаток алгоритма Миллера

Как было выше описано, алгоритм Миллера основывается на том, что для простого числа не существует свидетелей простоты по Миллеру на отрезке от $[2; f(N)]$.

Несмотря на то, что для доказательства простоты числа *N* рассматриваются числа на достаточно небольшом отрезке, алгоритм Миллера на много порядков медленнее, чем вероятностный алгоритм Миллера-Рабина (например, для 1024-битного числа необходимо проверять число для всех простых оснований до 1007582 и кроме того, в пункте *2.б)* это число необходимо возводить в степень *N – 1*)

Алгоритм Миллера – Рабина

Алгоритм Миллера – Рабина является модификацией алгоритма Миллера, с помощью которого можно достаточно эффективно определить, является ли данное число составным. Однако, с его помощью нельзя строго доказать простоту числа.

Псевдокод

Ввод числа n

Если $n \neq m^s, m, s \in Z \geq 2$, то

$\mathrm{f} = 2 * (\ln n)^2$

Для всех $a \leq f$, где a – простое:

Если $n \; mod \; a \neq 0$ и

Если $a^{n-1} \neq 1 \; (mod \; n)$ и

Если для $k = \max(k \in N, 2^k | (N-1) : 1 < \text{НОД}\left(a^{\frac{n-1}{2^k}} - 1 (mod \; n), n\right) < n$

то n – простое

иначе n - составное

Тест Миллера – Рабина

Пусть $N > 2$. Представим число $N - 1$ в виде $N - 1 = 2^s * d$, где d – нечетно. Тогда если N – простое число, то для любого $1 \leq a \leq N$, $a \in Z$ выполняется одно условий:

1. $a^d \equiv 1 \ (mod\ N)$
2. $\exists r, 0 \leq r \leq s: a^{2^r * d} \equiv -1 \ (mod\ N)$

Пример

1. $221 = 2^2 * 55$
2. Для a = 174: $174^{2^0 * 55} \; mod \; 221 = 47 \neq 220$

$174^{2^1 * 55} \; mod \; 221 = 220 = 220$

Для a = 137: $137^{2^0 * 55} \; mod \; 221 = 188 \neq 220$

$137^{2^1 * 55} mod \; 221 = 205 \neq 220$

$137^{2^2 * 55} mod 221 = 86 \neq 220$

Использованная литература

О. Н. Василенко «Теоретико – числовые алгоритмы в криптографии»

В. В. Ященко «Введение в криптографию»

https://ru.wikipedia.org/wiki/Тест_Миллера_—_Рабина#cite_ref-Baillie.2C_Wagstaff.E2.80.941980.E2.80.94.E2.80.94_9-0

https://ru.wikipedia.org/wiki/Тест_Миллера_(теория_чисел)#.D0.9F.D1.80.D0.B8.D0.BD.D1.86.D0.B8.D0.BF_.D1.80.D0.B0.D0.B1.D0.BE.D1.82.D1.8B

https://ru.wikipedia.org/wiki/Гипотеза_Римана

Благодарю за внимание!