МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Проверка чисел на простоту с помощью малой теоремы Ферма

ЛАБОРАТОРНАЯ РАБОТА

студента 4 курса 431 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Серебрякова Алексея Владимировича

Научный руководитель

доцент, к. п. н. _____ А. С. Гераськин

подпись, дата

Саратов 2021

Описание алгоритма

Содержание [править | править код]

Если *n* — простое число, то оно удовлетворяет сравнению $a^{n-1} \equiv 1 \pmod{n}$ для любого *a*, которое не делится на *n*.

Выполнение сравнения $a^{n-1} \equiv 1 \pmod{n}$ является необходимым, но не достаточным признаком простоты числа. То есть, если найдётся хотя бы одно *a*, для которого $a^{n-1} \not\equiv 1 \pmod{n}$, то число *n* — составное; в противном случае ничего сказать нельзя, хотя шансы на то, что число является простым, увеличиваются. Если для составного числа *n* выполняется сравнение $a^{n-1} \equiv 1 \pmod{n}$, то число *n* называют **псевдопростым по основанию *a***. При проверке числа на простоту тестом Ферма выбирают несколько чисел *a*. Чем больше количество *a*, для которых $a^{n-1} \equiv 1 \pmod{n}$, тем больше шансы, что число *n* простое. Однако существуют составные числа, для которых сравнение $a^{n-1} \equiv 1 \pmod{n}$ выполняется для всех *a*, взаимно простых с *n* — это числа Кармайкла. Чисел Кармайкла — бесконечное множество, наименьшее число Кармайкла — 561. Тем не менее, тест Ферма довольно эффективен для обнаружения составных чисел.

Код программы

```
#include <bits/stdc++.h>
#include <iostream>

using namespace std;

int validated_input()
{
   int s = 0;
   while (!(cin >> s))
   {
      cin.clear();
      cin.ignore(numeric_limits<streamsize>::max(), '\n');
      printf("! Неверный ввод. Повторите ввод, начиная с первого неверного элемента.\n");
   }

   return s;
}

int mul(int a, int b, int m)
{

   if (b == 1)
      return a;

   if (b % 2 == 0)
   {
      int t = mul(a, b / 2, m);
      return (2 * t) % m;
   }

   return (mul(a, b - 1, m) + a) % m;
}

int pows(int a, int b, int m)
{

   if (b == 0)
      return 1;

   if (b % 2 == 0)
   {
      int t = pows(a, b / 2, m);
      return mul(t, t, m) % m;
   }

   return (mul(pows(a, b - 1, m), a, m)) % m;
}
```

```
int gcd(int a, int b)
{
   return b ? gcd(b, a % b) : a;
}

bool test(int p, int n)
{

   if (p == 2)
      return true;

   for (int i = 1; i <= n; i++)
   {
      int a = (rand() % (p - 2)) + 2;
      printf(i % 10 == 1 ? "\n [a = %4d]" : " [a = %4d]", a);

      if (gcd(a, p) != 1)
         return false;

      if (pows(a, p - 1, p) != 1)
         return false;

   }

   return true;
}

int main()
{
   setlocale(0, "");
   int p, n;

   printf("\nТеорема Ферма: Если p - прсотое и a - целое число, не кратное p, то:\n    ");
   printf("a^(p-1) - 1\nделится на p\n");

   printf("\nВведите число p: ");
   p = validated_input();

   printf("\nВведите количество проверок n: ");
   n = validated_input();

   bool t = test(p, n);

   t ? printf("\nЧисло %d - является простым\n", p) : printf("\nЧисло %d - не является простым\n", p);

   return 0;
}
```

Пример запуска программы

```
 *  Executing task: /bin/bash -c ./build/Debug/outDebug

Теорема Ферма: Если p - прсотое и a - целое число, не кратное p, то:
    a^(p-1) - 1
делится на p

Введите число p: 571

Введите количество проверок n: 1000

 [a =  58] [a = 562] [a =  192] [a =  368] [a =  306] [a =  472] [a =  244] [a =  187] [a =  380] [a =  121] [a =  355] [a =  393] [a =  218] [a =   56] [a =  529] [a =  123] [a =  464] [a =  284] [a =  211] [a =  211]
[a =  333] [a =  467] [a =  399] [a =  463] [a =  152] [a =  490] [a =  490] [a =  154] [a =  256] [a =  198] [a =  487] [a =   48] [a =  190] [a =  413] [a =  150] [a =  230] [a =  314] [a =  393] [a =  151] [a =  133]
[a =  248] [a =  504] [a =  250] [a =  464] [a =  294] [a =  514] [a =  322] [a =  187] [a =  532] [a =  531] [a =  133] [a =  294] [a =  164] [a =  530] [a =  187] [a =  314] [a =  185] [a =  411] [a =  466] [a =  175]
[a =   38] [a =  382] [a =  222] [a =  226] [a =  530] [a =  106] [a =  190] [a =  273] [a =  233] [a =  339] [a =  131] [a =  216] [a =    8] [a =  379] [a =  109] [a =  301] [a =   58] [a =  165] [a =  222] [a =   20]
[a =  431] [a =   89] [a =  312] [a =   24] [a =   48] [a =  233] [a =   72] [a =  232] [a =   73] [a =  536] [a =  405] [a =  110] [a =   83] [a =  361] [a =   70] [a =   42] [a =  202] [a =  259] [a =   50] [a =  433]
[a =  332] [a =  484] [a =   78] [a =  339] [a =   28] [a =  491] [a =  374] [a =   85] [a =  390] [a =  330] [a =  103] [a =  555] [a =  418] [a =  149] [a =  313] [a =  200] [a =  381] [a =  383] [a =  166] [a =  452]
[a =   84] [a =  306] [a =  296] [a =  166] [a =   96] [a =  365] [a =  511] [a =   32] [a =  358] [a =  295] [a =  200] [a =  424] [a =  208] [a =   12] [a =  497] [a =  235] [a =  237] [a =  300] [a =   54] [a =   57]
[a =  365] [a =  155] [a =  346] [a =  212] [a =   38] [a =   89] [a =  410] [a =  417] [a =  470] [a =    6] [a =   35] [a =  553] [a =   46] [a =   65] [a =  453] [a =  445] [a =  164] [a =  129] [a =  476] [a =  520]
[a =  423] [a =  105] [a =  110] [a =  365] [a =  115] [a =   36] [a =   29] [a =   87] [a =  335] [a =  386] [a =  142] [a =  434] [a =  275] [a =  486] [a =   75] [a =  312] [a =  309] [a =  219] [a =  158] [a =  209]
[a =  528] [a =  496] [a =  496] [a =    3] [a =  560] [a =  114] [a =  447] [a =  153] [a =  241] [a =  352] [a =  408] [a =   93] [a =  191] [a =  516] [a =  193] [a =   40] [a =  550] [a =  220] [a =  125] [a =   50]
[a =   36] [a =  570] [a =  482] [a =  309] [a =  222] [a =  291] [a =  355] [a =  529] [a =  509] [a =  248] [a =  472] [a =  202] [a =  173] [a =  133] [a =  204] [a =  467] [a =  245] [a =  385] [a =  355] [a =  485]
[a =  471] [a =  192] [a =  312] [a =   91] [a =  442] [a =  503] [a =  434] [a =  157] [a =  458] [a =  294] [a =  206] [a =  228] [a =   29] [a =  422] [a =  271] [a =  554] [a =  448] [a =   56] [a =  513] [a =  122]
[a =  302] [a =  150] [a =  322] [a =  209] [a =  282] [a =  260] [a =  106] [a =  261] [a =   74] [a =  459] [a =  175] [a =  543] [a =  385] [a =  222] [a =  368] [a =  256] [a =  154] [a =  537] [a =  411] [a =  346]
[a =  260] [a =  351] [a =    3] [a =   23] [a =  508] [a =    9] [a =    7] [a =  385] [a =   63] [a =  254] [a =  241] [a =   99] [a =  402] [a =  561] [a =  306] [a =  418] [a =  251] [a =  146] [a =  109] [a =   59]
[a =   34] [a =   18] [a =   32] [a =  153] [a =  238] [a =  134] [a =  407] [a =  391] [a =  100] [a =  553] [a =  471] [a =   94] [a =   69] [a =  473] [a =  116] [a =    6] [a =  480] [a =  426] [a =  125] [a =  277]
[a =  109] [a =  364] [a =  374] [a =  509] [a =   91] [a =  414] [a =   93] [a =   76] [a =  559] [a =  200] [a =  133] [a =  327] [a =  216] [a =  468] [a =  215] [a =  453] [a =   32] [a =  356] [a =    9] [a =  435]
[a =  338] [a =  478] [a =  264] [a =  142] [a =  116] [a =  114] [a =  451] [a =  330] [a =  538] [a =    6] [a =   36] [a =   76] [a =  104] [a =  144] [a =  319] [a =  498] [a =  293] [a =  410] [a =    3] [a =   17]
[a =  344] [a =  440] [a =   78] [a =  559] [a =  337] [a =  291] [a =  177] [a =  103] [a =   77] [a =  184] [a =  537] [a =  149] [a =  396] [a =  230] [a =  289] [a =  247] [a =  342] [a =  170] [a =    6] [a =   45]
[a =  479] [a =  346] [a =  119] [a =  317] [a =  224] [a =  172] [a =  245] [a =  515] [a =   12] [a =  551] [a =  530] [a =   90] [a =  420] [a =  343] [a =   78] [a =  187] [a =   63] [a =  558] [a =  288] [a =  138]
[a =  476] [a =  559] [a =  286] [a =  302] [a =  523] [a =  309] [a =  547] [a =   30] [a =  213] [a =  287] [a =   73] [a =  121] [a =   62] [a =  495] [a =  173] [a =   21] [a =   97] [a =  416] [a =  534] [a =  412]
[a =  132] [a =  230] [a =  500] [a =  551] [a =    2] [a =  313] [a =  472] [a =   63] [a =  300] [a =  494] [a =  505] [a =  206] [a =  483] [a =  525] [a =  242] [a =  435] [a =  568] [a =  523] [a =  464] [a =  211]
[a =  239] [a =  271] [a =  330] [a =   36] [a =  196] [a =  501] [a =   55] [a =  291] [a =   82] [a =  323] [a =  437] [a =  213] [a =  551] [a =  366] [a =  498] [a =  287] [a =  413] [a =  399] [a =   85] [a =  143]
[a =  322] [a =   19] [a =   83] [a =  539] [a =  278] [a =  323] [a =  140] [a =  275] [a =  275] [a =  338] [a =  484] [a =  248] [a =   38] [a =  549] [a =  282] [a =  232] [a =  215] [a =  335] [a =  257] [a =  296]
[a =   88] [a =  123] [a =  243] [a =  373] [a =  224] [a =  475] [a =   90] [a =   66] [a =  303] [a =  173] [a =  512] [a =  359] [a =  495] [a =   24] [a =  328] [a =  202] [a =   81] [a =  202] [a =  211] [a =  354]
[a =  538] [a =  125] [a =   32] [a =    5] [a =  400] [a =   48] [a =  541] [a =   52] [a =  382] [a =  227] [a =   82] [a =  204] [a =   85] [a =  323] [a =    6] [a =   43] [a =  227] [a =  399] [a =  412] [a =  264]
[a =  570] [a =  354] [a =   53] [a =  230] [a =  112] [a =  115] [a =  430] [a =  192] [a =  315] [a =   71] [a =  280] [a =  282] [a =  499] [a =  310] [a =   21] [a =  336] [a =  357] [a =  560] [a =  386] [a =  473]
[a =  522] [a =  467] [a =  106] [a =  341] [a =  524] [a =  415] [a =  382] [a =  486] [a =  244] [a =  223] [a =  484] [a =  548] [a =  311] [a =  271] [a =  208] [a =  422] [a =  384] [a =  372] [a =  348] [a =  433]
[a =  177] [a =   57] [a =  449] [a =  410] [a =  102] [a =  205] [a =  175] [a =  193] [a =  194] [a =  296] [a =  400] [a =  450] [a =  497] [a =  240] [a =  220] [a =  186] [a =   84] [a =  336] [a =  406] [a =   62]
[a =  294] [a =  320] [a =  345] [a =   34] [a =   20] [a =  551] [a =  190] [a =  139] [a =   88] [a =  536] [a =  306] [a =  569] [a =  328] [a =  185] [a =  408] [a =  164] [a =  388] [a =   13] [a =  355] [a =  316]
[a =   43] [a =  184] [a =  196] [a =  538] [a =  422] [a =  150] [a =  458] [a =  240] [a =  221] [a =  294] [a =  301] [a =  513] [a =   43] [a =   75] [a =  281] [a =  366] [a =  360] [a =  470] [a =  503] [a =  182]
[a =  171] [a =  239] [a =  180] [a =  233] [a =  158] [a =   18] [a =  395] [a =  280] [a =  334] [a =  484] [a =   25] [a =  375] [a =  402] [a =  524] [a =   78] [a =  558] [a =  409] [a =  270] [a =  228] [a =   59]
[a =  562] [a =  263] [a =  306] [a =  339] [a =   72] [a =   16] [a =  440] [a =  166] [a =  220] [a =  372] [a =  346] [a =  390] [a =  345] [a =  525] [a =  357] [a =  237] [a =  277] [a =  182] [a =  515] [a =   40]
[a =  400] [a =  275] [a =  149] [a =  232] [a =  228] [a =  530] [a =  219] [a =  371] [a =  229] [a =  181] [a =  428] [a =  526] [a =  442] [a =  163] [a =   30] [a =  248] [a =  483] [a =  468] [a =  412] [a =  132]
[a =    6] [a =  493] [a =  520] [a =   85] [a =  183] [a =   43] [a =  321] [a =  458] [a =  223] [a =  570] [a =  232] [a =  357] [a =  274] [a =  115] [a =   10] [a =  237] [a =  379] [a =  236] [a =   37] [a =  342]
[a =  151] [a =  200] [a =  257] [a =   23] [a =   97] [a =  326] [a =    5] [a =    9] [a =  528] [a =  416] [a =  140] [a =  532] [a =  338] [a =  394] [a =   47] [a =  255] [a =  435] [a =  366] [a =  142] [a =  392]
[a =  365] [a =  108] [a =  179] [a =  374] [a =  221] [a =  500] [a =   40] [a =  334] [a =  470] [a =  380] [a =  105] [a =   51] [a =    9] [a =  137] [a =   72] [a =  105] [a =  197] [a =   75] [a =  417] [a =  154]
[a =  225] [a =  291] [a =  116] [a =  297] [a =  115] [a =  161] [a =  550] [a =  284] [a =  261] [a =  426] [a =  411] [a =  360] [a =  532] [a =  324] [a =  163] [a =  487] [a =  253] [a =  506] [a =  250] [a =  153]
[a =  316] [a =  354] [a =  202] [a =   59] [a =  489] [a =    8] [a =  467] [a =  115] [a =  386] [a =  314] [a =    3] [a =   41] [a =   34] [a =  117] [a =   72] [a =  452] [a =   12] [a =   52] [a =  471] [a =    7]
[a =  212] [a =  311] [a =  366] [a =  174] [a =   64] [a =  263] [a =   90] [a =  315] [a =  504] [a =   75] [a =  202] [a =  554] [a =  163] [a =  402] [a =   42] [a =   81] [a =  408] [a =  508] [a =  499] [a =  529]
[a =  556] [a =  500] [a =  568] [a =  324] [a =  352] [a =  374] [a =  206] [a =  362] [a =  160] [a =  106] [a =  368] [a =  371] [a =  151] [a =  468] [a =  543] [a =  518] [a =  465] [a =  367] [a =  262] [a =  398]
[a =  176] [a =  463] [a =  381] [a =  337] [a =   30] [a =  158] [a =  416] [a =  173] [a =   95] [a =   80] [a =  131] [a =   80] [a =   10] [a =  433] [a =  402] [a =  360] [a =  236] [a =  342] [a =  456] [a =  395]
[a =  182] [a =  558] [a =  195] [a =   67] [a =  191] [a =  472] [a =   14] [a =   86] [a =    4] [a =  275] [a =  218] [a =  179] [a =  472] [a =  334] [a =  514] [a =  500] [a =  490] [a =   96] [a =  407] [a =  319]
[a =  174] [a =  536] [a =  133] [a =  487] [a =  398] [a =  269] [a =   12] [a =   64] [a =  346] [a =  467] [a =  193] [a =  526] [a =  454] [a =  386] [a =   23] [a =   75] [a =   23] [a =  340] [a =  464] [a =   25]
[a =   44] [a =  416] [a =  202] [a =  250] [a =  179] [a =  146] [a =  485] [a =  403] [a =  240] [a =  321] [a =  151] [a =  148] [a =  287] [a =   18] [a =   65] [a =  419] [a =  286] [a =   75] [a =  481] [a =   61]
[a =  540] [a =  103] [a =  321] [a =  160] [a =  223] [a =   78] [a =  538] [a =  244] [a =  417] [a =  167] [a =  268] [a =  195] [a =   12] [a =  204] [a =  180] [a =  190] [a =  348] [a =   94] [a =  327] [a =  322]
[a =  149] [a =  213] [a =  469] [a =  170] [a =  229] [a =  268] [a =   19] [a =  249] [a =  341] [a =  498] [a =   44] [a =   47] [a =  336] [a =  364] [a =  510] [a =  293] [a =  176] [a =  477] [a =  536] [a =  327]
[a =   73] [a =  538] [a =  521] [a =   83] [a =  171] [a =  435] [a =   71] [a =  254] [a =  527] [a =  333] [a =  310] [a =  410] [a =  544] [a =  513] [a =   10] [a =  507] [a =  210] [a =   27] [a =  186] [a =  286]
[a =  259] [a =  228] [a =  331] [a =  329] [a =  326] [a =  270] [a =   52] [a =  237] [a =  481] [a =  322] [a =  562] [a =  280] [a =  288] [a =  248] [a =  369] [a =  194] [a =  112] [a =  111] [a =  182] [a =  373]
[a =  178] [a =  491] [a =  213] [a =  456] [a =  433] [a =  221] [a =  392] [a =  378] [a =  246] [a =  312] [a =   93] [a =  239] [a =  275] [a =  422] [a =  567] [a =   30] [a =  426] [a =   48] [a =  570] [a =   72]
[a =  368] [a =  562] [a =  358] [a =  391] [a =  544] [a =  156] [a =  319] [a =   86] [a =  570] [a =  500] [a =  457] [a =  177] [a =  156] [a =  404] [a =   62] [a =  323] [a =   54] [a =  189] [a =  130] [a =   34]
Число 571 - является простым
 *  Terminal will be reused by tasks, press any key to close it.
```

```
 *  Executing task: /bin/bash -c ./build/Debug/outDebug

Теорема Ферма: Если p - прсотое и a - целое число, не кратное p, то:
    a^(p-1) - 1
делится на p

Введите число p: 1105

Введите количество проверок n: 1000

 [a =  882] [a =   59] [a =  520] [a =  520]
Число 1105 - не является простым
 *  Terminal will be reused by tasks, press any key to close it.
```