Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе №3»**

«Основы теории чисел и их использование в криптографии»

**Выполнил:** студент 3 курса

4 группы специальности ПОИТ

Супрунюк Евгений Андреевич

**Проверил:** преподаватель

Сазонова Дарья Владимировна

Минск 2023

**Найти все простые числа в интервале [2, n]. Значение n соответствует варианту из табл. 1.2, указанному преподавателем. Подсчитать количество простых чисел в указанном интервале. Сравнить это число с n/ln(n):**

Реализация на языке C++:

|  |
| --- |
| // A function to check if a number is prime or not  bool is\_prime(int n)  {  // If the number is less than 2, it is not prime  if (n < 2) {  return false;  }    // If the number is divisible by any number from 2 to its square root, it is not prime  for (int i = 2; i \* i <= n; i++)  {  if (n % i == 0)  return false;  }    // Otherwise, the number is prime  return true;  } |

|  |
| --- |
| // A function to print all the prime numbers in a given range  int print\_primes(int low, int high)  {  int count = 0;  // Loop through the range and check each number for primality  for (int n = low; n <= high; n++)  {  if (is\_prime(n))  {  // If the number is prime, print it  std::cout << n << " ";  count++;  }  }  std::cout << "\nCount of prime numbers = " << count << "\n";  return count;  } |

Полученный результат:

|  |
| --- |
| 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409  Count of prime numbers = 80  n/ln(n) = 68.2884 |

**Повторить п. 1 для интервала [m, n]. Сравнить полученные результаты с «ручными» вычислениями, используя «решето Эратосфена».**

Полученная энтропия:

|  |
| --- |
| 379 383 389 397 401 409  Count of prime numbers = 6  n/ln(n) = 68.2884 |

**Функция вычисления НОД двух чисел:**

|  |
| --- |
| // A function to return the GCD of two numbers using Euclid's algorithm  int gcd(int a, int b)  {  // If one of the numbers is zero, the other is the GCD  if (a == 0)  return b;  if (b == 0)  return a;  if (a == b)  return a;  // If one number is greater than the other, subtract the smaller from the larger and repeat  return a > b ? gcd(a - b, b) : gcd(a, b - a);  } |

**Пример вычисления НОД двух чисел:**

|  |
| --- |
| Enter two numbers:  280  576  The GCD of 280 and 576 is 8 |

**Пример вычисления НОД трёх чисел:**

|  |
| --- |
| Enter three numbers:  66  27  18  The GCD of 66 and 27 and 18 is 3 |