Оглавление

[Простые числа 2](#_Toc498156878)

[**Решето Эратосфена [2]** 12](#_Toc498156879)

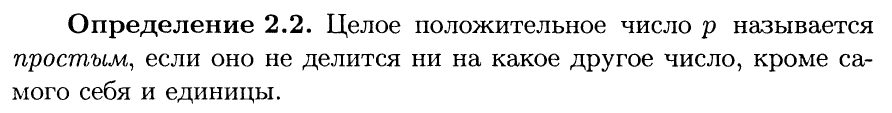
[Литература 13](#_Toc498156880)

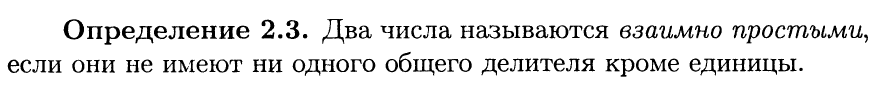
# Простые числа

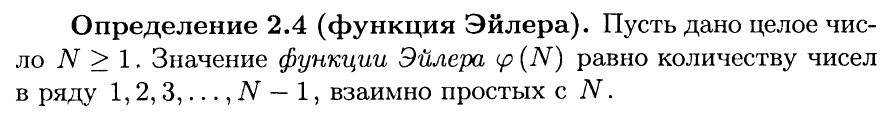
Простые числа играют чрезвычайно важную роль в обеспечении компьютерной безопасности. Ассиметричная криптография невозможна без использования простых чисел

Один из ключевых моментов в ассиметричной криптографии – использование специальных алгоритмов, позволяющих получить простое число заданной размерности (заданное количество бит в бинарном представлении).

Приведенные ниже определения взяты из [2].



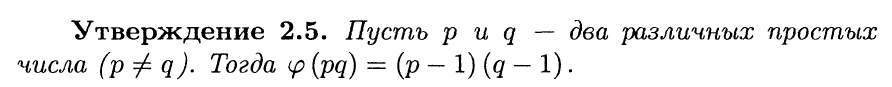




|  |
| --- |
| **Задание 1.** Написать функцию euler\_fun(n) – функцию Эйлера. Проверить, что |



|  |
| --- |
| **Задание 2.** Записать доказательство этого утверждения. |

****

|  |
| --- |
| **Задание 3.** Записать доказательство этого утверждения. |

Числа , называются сравнимыми по модулю  (записывается как ), если их разность  делится на . Сравнимость по модулю  разбивает множество целых чисел на непересекающиеся классы сравнимых по модулю  чисел. Эти классы называются классами вычетов по модулю . Принято обозначать совокупность классов вычетов по модулю  как  или . Множество  классов вычетов по модулю  с операциями сложения и умножения образует коммутативное кольцо с единицей. Класс вычетов, содержащий число  обозначается  или .

Кольцо  является полем тогда и только тогда, когда  - простое число.

|  |
| --- |
| Пример |

Обозначим  множество вычетов  таких, что НОД(x,n)=1:



|  |
| --- |
| Пример: |

Это означает, что для каждого элемента из существует его обратный относительно операции умножения. Тогда,  называют еще мультипликативной группой кольца  или группой обратимых элементов этого кольца.

|  |
| --- |
| **Задание 4.** Написать функцию z\_nz\_group(n), которая возвращает элементы мультипликативной группы |

*Порядок группы*  – это число элементов в ней, обозначается .

Группа  называется *циклической*, если в ней существует элемент  такой, что любой элемент  является его степенью, т.е.



Тогда, говорят, что  порождается , т.е. , а сам  называют порождающим.

|  |
| --- |
| **Задание 5**. Проверьте, что      Группа не циклическая. |

Пусть  и  взаимно простые числа, тогда *порядком числа*  по модулю  называется наименьшее натуральное число , такое что



Порядок числа  обозначается через , т.е. .

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Задание 6**. Для  заполнить таблицу   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1 | 2 | 4 | 5 | 7 | 8 | |  | 1 | 6 | 3 | 6 | 3 | 2 | |

Порядок группы  - равен .

|  |
| --- |
| **Задание 7**. Написать функцию multiplicative\_order(g,n), которая возвращает порядок элемента g в . |

**Утверждение 1**: Порядок любого элемента  из  является делителем . Данное утверждение является следствием хорошо известной в теории групп теоремы Лагранжа, которая гласит: порядок элемента конечной группы делит порядок самой группы.

|  |
| --- |
| **Задание 8**. Проверить данное утверждение для . |

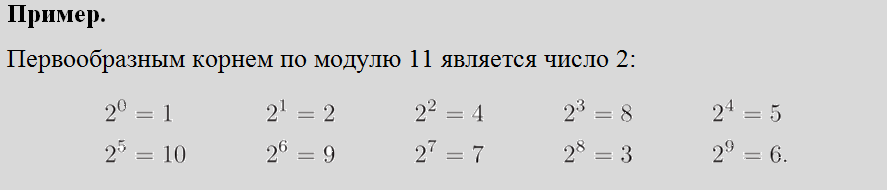
**Утверждение 2**: Более того, порядок любого элемента  из  является делителем : . В частности, порядок делит и .

|  |
| --- |
| В самом деле, пусть  Дано: . Разделим  на :    Тогда    Но , а  - порядок числа , т.е. наименьшее натуральное число, такое что  Следовательно, . Это означает, что  делит . |

Если порядок элемента  равен , то число g называется *первообразным корнем* по модулю .

Пусть  - простое число. Тогда первообразным корнем по модулю  является число g, порядок которого равен :





|  |
| --- |
| **Пример.**  Число 2 не является первообразным корнем по модулю 17:    Число 3 является первообразным корнем по модулю 17: |

|  |
| --- |
| **Задание 9**. Написать функцию primitive\_roots(n), которая среди всех элементов  находит все первообразные корни.  print(primitive\_roots(4))  >>[3]  print(primitive\_roots(7))  >>[3, 5]  print(primitive\_roots(29))  >>[2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27] |

Вопрос о наличии первообразных корней по модулю – это вопрос о том, будет ли группа  циклической. Следующее утверждение было впервые доказано Гауссом: если модуль  есть простое число , то первообразные корни существуют. Теорема Гаусса может быть сформулирована так: мультипликативная группа поля из  элементов является циклической.

**Утверждение 3**: Число g является первообразным корнем по простому модулю  тогда и только тогда, когда

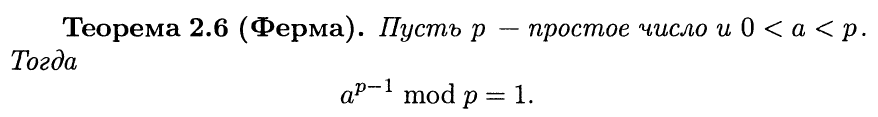


Для любого простого делителя  числа .

**Утверждение 4**: В ровно  первообразных корней.

|  |
| --- |
| **Задание 10**. Проверить данное утверждение для . |

|  |
| --- |
| **Задание 11**. Более общее утверждение: если  делит  то существует  элементов порядка . Проверить для . |



Можно встретить и такую запись:

 (1)

Что означает еще и то, что  делится на .

|  |
| --- |
| **Задание 12.** Проверьте с помощью функции pow(): |

Указанный в формулировке диапазон значений  означает, что  является взаимно простым с .

|  |
| --- |
| **Задание 13.** Проверьте, что соотношение верно и при , если  и  – взаимно простые числа. |

|  |
| --- |
| **Задание 14.** Записать доказательство теоремы. |

Малая теорема Ферма в более общей формулировке: Пусть  - простое число, - любое целое.

Тогда

 (2)

Что означает еще и то, что  делится на .

|  |
| --- |
| **Задание 15.** Проверить указанное в теореме соотношение (2) с помощью функции pow(). |

|  |
| --- |
| **Задание 16.** Записать доказательство теоремы в записи (2). |

Малую теорему Ферма можно использовать для нахождения обратного значения по умножению:

 (3)

|  |
| --- |
| **Задание 17.** Найти обратное значение для  = 7814 в . Два способа:   1. Расширенный алгоритм Евклида 2. Формула (3) |

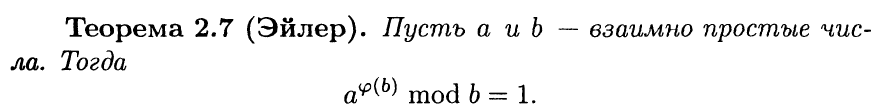
|  |
| --- |
| **Задание 18.** Найдите не простое число, с которым выполняется соотношение (1), как в этом примере: |

Если необходимо определить является ли число простым, то надо, например, проверить выполнение соотношения (1). Если оно выполнилось, это еще не означает, что проверяемое число – простое. Надо выполнять проверку много раз:



Теперь можно утверждать, что 25 – не простое.

Элементы такой проверки положены в основу алгоритма проверки чисел на простоту (тест Рабина-Миллера).



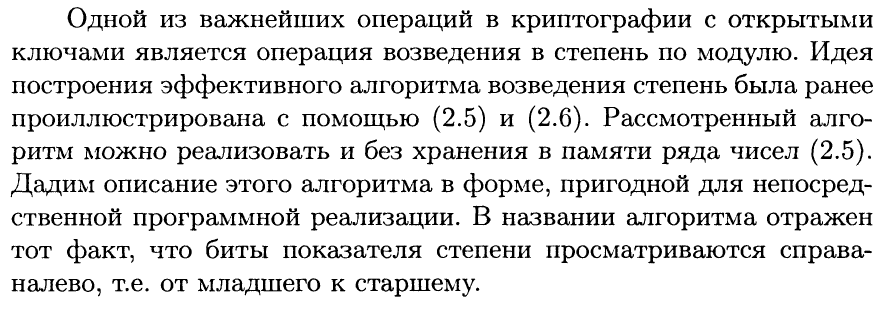
Можно встретить и такую запись:

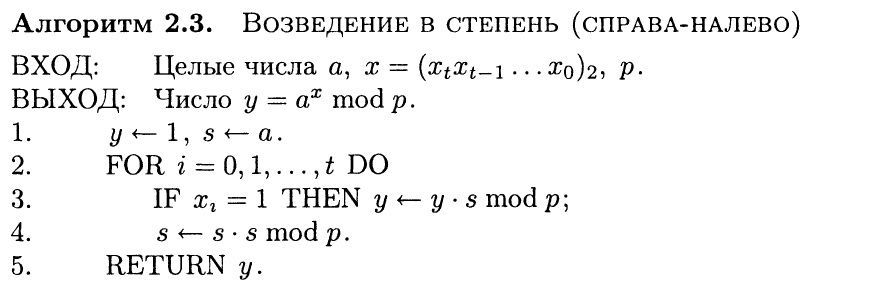


Теорем Эйлера является частным случаем теоремы Ферма, когда - простое число.

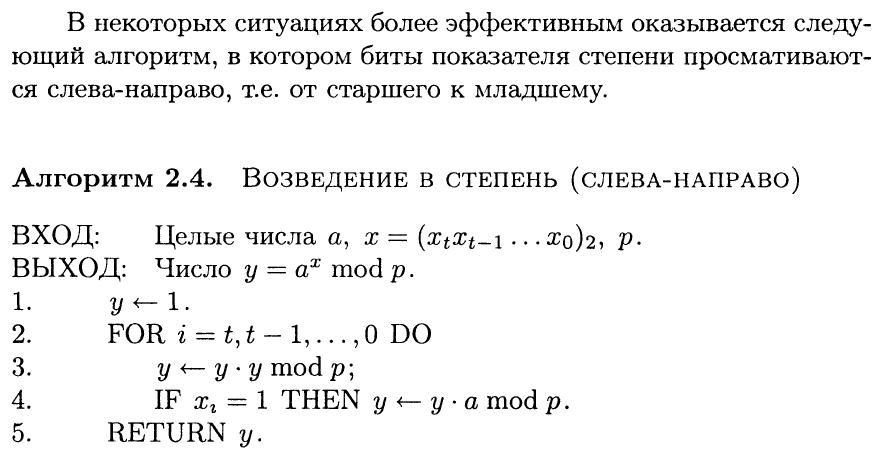
|  |
| --- |
| **Задание 19.** Проверить, используя функции euler\_fun() и pow(): |

|  |
| --- |
| **Задание 20.** Записать доказательство теоремы Эйлера. |



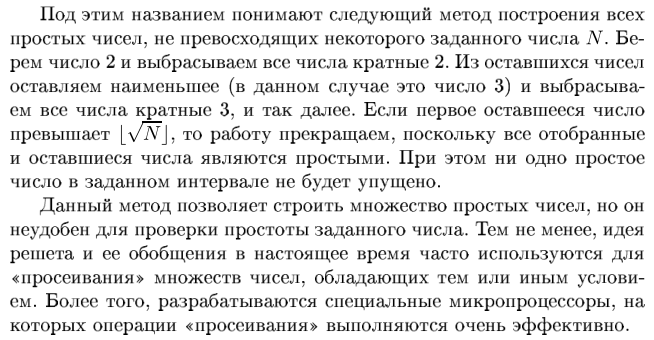


|  |
| --- |
| **Задание 21.** Написать функцию pow\_right\_left(), которая реализует алгоритм 2.3. |



|  |
| --- |
| **Задание 22.** Написать функцию pow\_left\_right (), которая реализует алгоритм 2.4. |

**Решето Эратосфена [2]**



|  |
| --- |
| **Задание 23.** Написать функцию sieveEratosthen(), которая реализует алгоритм решето Эратосфена:  print(sieveEratosthen(120))  >> [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] |

|  |
| --- |
| **Задание 24. Записать решение упражнений 2.6, 2.7, 2.8, 2.13, 2,14 a), 2.15 а), 2.16 а) из [1].** |

# Литература

[1] Рябко Б.Я., Фионов А.Н., Криптографические методы защиты информации: учебное пособие для вузов. – М.: Горячая линия-Телеком, 2005. – 229 с.

[2] Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002. – 104 с.

[3] Stallings W, “Cryptography And Network Security. Principles And Practice”, 5th Edition, 2011.