МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ НА ТЕМУ:**

**Основы теории чисел и их использование в криптографии**

Ф.И.О.

Савельев Дмитрий Витальевич

Преподаватель

Берников Владислав Олегович

Минск 2021

**Цель:** приобретение практических навыков выполнения операций с числами для решения задач в области криптографии и разработка приложений для автоматизации этих операций.

**Задачи:**

1. Закрепить теоретические знания по высшей арифметике.

2. Научиться практически решать задачи с использованием простых и взаимно простых чисел, вычислений по правилам модулярной арифметики и нахождению обратных чисел по модулю.

3. Разработать приложение для реализации указанных преподавателем операций с числами.

4. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения эксперимента с использованием приложения и результатов эксперимента.

# 1. Теоретические сведения

В основе современной криптографии лежит теория чисел. Теория чисел, или высшая арифметика, – раздел математики, изучающий натуральные числа и иные похожие величины. В зависимости от используемых методов в теории чисел рассматривают несколько направлений. Нас будут интересовать вопросы делимости целых чисел, вычисления наибольшего общего делителя (НОД), разложение числа на простые множители, малая теорема Ферма́, теорема Эйлера, элементы теории вычетов.

# 1.1. Основные понятия и определения

**Определение 1.** Множество всех целых чисел (обозначим буквой Z) есть набор всех действительных чисел без дробной части: {..., –3, –2, –1, 0, 1, 2, 3, ...}.

**Определение 2.** Натуральные числа являются подмножеством целых чисел и образуют множество N: {1, 2, 3, ...}.

**Определение 3.** Делимость – одно из основных понятий теории чисел. Если для некоторого целого числа a и натурального числа b существует целое число q, при котором bq = a, то говорят, что число a делится на b. В этом случае b называется делителем числа a, а a называется кратным числу b. При этом используются следующие обозначения: a ⋮ b – a делится на b, или b | a – b делит a. Из последнего определения следует, что:

• любое натуральное число является делителем нуля;

• единица является делителем любого целого числа;

• любое натуральное число является делителем самого себя.

**Определение 4.** Делитель a называется собственным делителем числа b, если 1 < |a| < |b|, и несобственным – в противном случае.

**Определение 5.** Всякое целое число а можно представить с помощью положительного целого числа b равенством вида а = bq + r, 0 ≤ r ≤ b. Число q называется неполным частным, а число r – остатком отделения а на b.

# 1.2. Простые и составные числа

Каждое натуральное число, большее единицы, делится по крайней мере на два числа: на 1 и на само себя.

Если число не имеет делителей, кроме самого себя и единицы, то оно называется простым, а если у числа есть еще делители, то составным.

**Определение 6.** Натуральное число n называется простым, если n > 1 и не имеет положительных делителей, отличных от 1 и n. Простое число не делится без остатка ни на одно другое число.

Перечислим несколько важных свойств простых чисел.

*Свойство 1.* Любое составное число представляется уникальным образом в виде произведения простых чисел; иначе еще говорят, что разложение числа на простые множители однозначно. Это свойство вытекает из основной теоремы арифметики.

Основная теорема арифметики. Всякое натуральное число n, кроме 1, можно представить как произведение простых множителей:

|  |  |
| --- | --- |
|  | (1.1) |

Порядок записи сомножителей после последнего знака равенства соответствует канонической форме.

Для того чтобы представить относительно небольшое число в виде простых сомножителей, достаточно уметь делить числа столбиком. Однако при этом следует придерживаться некоторых простых правил. Для первого деления нужно выбрать наименьшее простое число, большее 1, которое делит исходное число без остатка. Частное от первого деления также нужно разделить с учетом указанных ограничений. Процесс деления продолжаем до тех пор, пока частным не будет 1.

*Свойство 2.* Простых чисел бесконечно много, причем существует примерно n / ln(n) простых чисел, меньших числа n.

*Свойство 3.* Наименьший простой делитель составного числа n не превышает √n, поэтому для проверки простоты числа достаточно проверить его делимость на 2 и на все нечетные (а еще лучше простые) числа, не превосходящие √n; как видим, данное свойство коррелирует со свойством 1 собственного делителя. Из соотношения n = qp натуральных чисел, больших единицы, следует, что либо p, либо q принадлежит отрезку от 2 до √n.

Поиск сомножителей числа n может вестись, например, перебором всех простых чисел до √n. Однако если множители – большие простые числа, то на их поиск может потребоваться много времени.

Сложность решения задачи разложения больших чисел на простые сомножители, известной как «проблема факторизации», определяет криптостойкость некоторых алгоритмов асимметричной криптографии, в частности алгоритма RSA.

*Свойство 4.* Любое четное число, большее 2, представимо в виде суммы двух простых чисел, а любое нечетное, большее 5, представимо в виде суммы трех простых чисел.

*Свойство 5.* Для любого натурального n, большего 1, существует хотя бы одно простое число на интервале от n до 2n.

**Определение 7.** Натуральное число n называется составным, если n > 1 и имеет по крайней мере один положительный делитель, отличный от 1 и n.

Единица не считается ни простым числом, ни составным.

Свойство 2 собственного делителя. Положительный наименьший собственный делитель составного числа n есть простое число.

Так как простое число не делится ни на какое другое, кроме себя самого, очевидный способ проверки числа n на простоту – разделить n на все числа (n – 1) и проанализировать наличие остатка от деления. Этот способ «в лоб» часто реализуется в компьютерных программах. Однако перебор может оказаться достаточно трудоемким, если на простоту нужно проверить число с количеством цифр в несколько десятков.

Существуют правила, способные заметно сократить время вычислений [4].

*Правило 1.* Воспользоваться свойством 3 простых чисел (см. выше).

*Правило 2.* Если последняя цифра анализируемого числа является четной, то это число заведомо составное.

*Правило 3.* Числа, делящиеся на 5, всегда оканчиваются пятеркой или нулем. Если младшим разрядом анализируемого числа являются 5 или 0, то такое число не является простым.

*Правило 4.* Если анализируемое число делится на 3, то и сумма его цифр тоже обязательно делится на 3.

*Правило 5.* Основано на свойстве делимости на 11. Нужно из суммы всех нечетных цифр числа вычесть сумму всех четных его цифр. Четность и нечетность определяется счетом от младшего разряда. Если получившаяся разность делится на 11, то и анализируемое число тоже на него делится.

*Правило 6*. Основано на свойстве делимости на 7 и 13. Нужно разбить анализируемое число на тройки цифр, начиная с младших разрядов. Просуммировать числа, стоящие на нечетных позициях, и вычесть из них сумму чисел на четных. Проверить делимость результата на числа 7 и 13.

**Определение 8.** Если два простых числа отличаются на 2, то их называют числами-близнецами.

Таких чисел не очень много. Например, ими являются 5 и 7, 29 и 31, 149 и 151.

Всякое натуральное число n > 1 либо является простым числом, либо имеет простой делитель.

Воспользуемся перечисленными свойствами для определения простоты числа 2009. Это число не делится на 2 (так как оно нечетно), не делится также на 3 (сумма его цифр 2 + 9 = 11 не делится на 3), не делится и на 5. Воспользуемся далее свойством 6: попробуем разделить 2009 на 7; в результате получается целый результат: 287. Таким образом, получен ответ: число 2009 – составное.

Понятно, что в криптографии используются числа, проверка на простоту которых производится гораздо дольше, и для работы с этими числами требуются специальные программные средства. К вопросу проверки чисел на простоту мы еще вернемся. Здесь же отметим, что первый алгоритм нахождения простых чисел, не превышающих n, был придуман Эратосфеном во II в. до н. э. и известен сейчас как «решето Эратосфена». Его суть в последовательном исключении из списка целых чисел от 1 до n (или из сокращенного диапазона, например от m до n, 1 < m ≤ n) чисел, кратных 2, 3, 5 и другим простым числам, уже найденным «решетом». Как видим, описанное выше свойство 2 простых чисел и положено в основу рассматриваемого алгоритма.

Для нахождения всех простых чисел не больше заданного числа n в соответствии с «решетом Эратосфена» нужно выполнить следующие шаги:

1) выписать подряд все целые числа от двух (либо от m) до n (2, 3, 4, …, n). Пусть некоторая переменная (например, s) изначально равна 2 – первому простому числу;

2) удалить из списка числа от 2s до n, считая шагами по s (это будут числа, кратные s: 2s, 3s, 4s, …);

3) найти первое из оставшихся чисел в списке, большее чем s, и присвоить значению переменной s это число;

4) повторять шаги 2 и 3, пока возможно.

Помимо рассмотренного алгоритма Эратосфена, который является наименее эффективным, в настоящее время разработаны и используются другие алгоритмы. Описание и программную реализацию этих алгоритмов можно найти, например, в известной и популярной у разработчиков криптографических приложений книге.

# 1.3. Взаимно простые числа и φ-функция

Понятие делимости чисел (см. определение 3) является одним из важных в теории чисел. С этим понятием, а также с его производным – общим делителем (см. определение 4) связаны другие важнейшие (в частности, для криптографии) понятия: наибольшего общего делителя (НОД) и взаимно простых чисел.

**Определение 9.** Наибольшее целое число, которое делит без остатка числа a и b, называется наибольшим общим делителем этих чисел – НОД (a, b).

Понятно, что значение НОД можно вычислять для неограниченного ряда чисел.

Простым и эффективным средством вычисления НОД (a, b) является алгоритм Евклида (примеры его использования приведены в [3]). В основе алгоритма лежит определение 5. В соответствии с этим определением используется цепочка вычислений двумя исходными (начальными) числами а и b:

|  |  |
| --- | --- |
|  | (1.2) |

При i = 0 в выражении (1.2) аi и bi соответствуют как раз числам а и b. Последний ненулевой остаток (ri, i ≥ 0) соответствует НОД (a, b).

Чтобы найти НОД нескольких чисел (например, a, b, c), достаточно найти НОД двух чисел (например, НОД (a, b) = d), потом НОД полученного (НОД (a, b)) и следующего числа (НОД (c, d)), и т. д.

Таким образом, чтобы вычислить НОД k чисел, нужно последовательно вычислить (k – 1) НОД. Последнее вычисление дает искомый результат.

**Определение 10.** Взаимно простыми являются целые числа, наибольший общий делитель которых равен 1.

**Теорема 1.** Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые числа u и v, что выполняется равенство

|  |  |
| --- | --- |
|  | (1.3) |

**Теорема 2.** Если НОД (a, b) = d, то справедливо следующее соотношение (соотношение Безу):

|  |  |
| --- | --- |
|  | (1.4) |

Формула (1.4) называется также реализацией «расширенного алгоритма Евклида». Этот алгоритм состоит из двух этапов: собственно алгоритма Евклида и вычислений на основе обратных подстановок или последовательного выражения остатков в каждом из шагов предыдущего этапа с соответствующим приведением подобных на каждом шаге.

Исследованием целых чисел занимался швейцарский математик Леонард Эйлер (Leonard Euler). Один из важных вопросов его исследования: сколько существует натуральных чисел, не превосходящих некоторое число n и взаимно простых с n? Ответ на этот вопрос связан с каноническим разложением числа n на простые множители (см. выше основную теорему арифметики и пример 4). Так, если

|  |  |
| --- | --- |
|  | (1.5) |

где p1, p2, ..., pn – разные простые множители, то число φ(n) натуральных чисел, не превосходящих n и взаимно простых с n, можно точно определить по формуле

|  |  |
| --- | --- |
|  | (1.4) |

Количество натуральных чисел, непревосходящих nивзаимно простых с n, называется функцией Эйлера и обозначается φ(n).

Если p – простое число, то φ(p) = p – 1, если числа p и q являются простыми и p ≠ q, то

|  |  |
| --- | --- |
|  | (1.4) |

# 1.4. Модулярная арифметика и обратные числа по модулю

Понятие «модулярная арифметика» ввел немецкий ученый К. Ф. Гаусс. В этой арифметике мы интересуемся остатком от деления числа а на число n (n – натуральное число и n > 1). Если таким остатком является число b, то можно записать:

a ≡ b (mod n), или a ≡ b mod n.

Такая формальная запись читается как «a сравнимо с b по модулю n».

При целочисленном (в том числе и нулевом) результате деления числа а на число n справедливо: a = b + kn.

Иногда b называют вычетом по модулю n, а числа a и b называют сравнениями (по модулю n).

Модулярная арифметика так же коммутативна, ассоциативна и дистрибутивна, как и обычная арифметика. В силу этих свойств сравнения можно почленно складывать, вычитать, умножать, возводить в степень (аm mod n ≡ (а mod n) m, если a ≡ b mod n, то am ≡ bm (mod n).

Указанные свойства позволяют упрощать сложность и время выполнения многих вычислений. Криптография использует множество вычислений по модулю n, потому что задачи типа вычисления дискретных логарифмов и квадратных корней очень трудны. Кроме того, с вычислениями по модулю удобнее работать, потому что они ограничивают диапазон всех промежуточных величин и результата.

Обратные числа в модулярной арифметике. Традиционное отношение чисел в арифметике: обратное к 7 равно 7–1 = 1/7, так как 7 · (1/7) = 1. В модулярной арифметике запись уравнения в виде

|  |  |
| --- | --- |
|  | (1.8) |

предусматривает поиск таких значений х и k, которые удовлетворяют равенству

|  |  |
| --- | --- |
|  | (1.9) |

Общая задача решения уравнения (1.8) может быть сформулирована следующим образом: найти такое х, что

|  |  |
| --- | --- |
|  | (1.10) |

Уравнение (1.10) имеет единственное решение, если а и n – взаимно простые числа, в противном случае – решений нет.

Уравнение (1.10) можно переписать в ином виде:

|  |  |
| --- | --- |
|  | (1.11) |

Если НОД (а, n) = 1, то а–1а ≡ 1 mod n, где а–1 – число, обратное а по модулю n. Справедливо также:

|  |  |
| --- | --- |
|  | (1.12) |

В силу приведенных рассуждений и обоснований выражению (1.12) удовлетворяют такие числа, при которых выполняется равенство

|  |  |
| --- | --- |
|  | (1.13) |

где k – целое число (результат деления xy/n).

Нахождение чисел, обратных по модулю, легко реализуется с помощью расширенного алгоритма Евклида.

Малая теорема Ферма. Если n – простое число, а число а не кратно n, то справедливо:

|  |  |
| --- | --- |
|  | (1.14) |

В соответствии с обобщением Эйлера приведенной теоремы, если НОД (а, n) = 1, то справедливо:

|  |  |
| --- | --- |
|  | (1.15) |

Последнее выражение можно переписать в следующем виде:

|  |  |
| --- | --- |
|  | (1.16) |

# 1.2. Практическое задание

Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

• вычислять НОД двух либо трех чисел;

• выполнять поиск простых чисел.

Для реализации вычисления НОДа двух либо трех чисел я использовал алгоритм Евклида.

Сначала пользователь должен определить количество чисел, для которых требуется вычислить НОД (доступны опции с 2 и 3 числами). Далее необходимо ввести исходные данные (числа n и m, если выбрана опция с 3 числами, то еще и l). Программа выведет на экран результат выполнения алгоритма Евклида (рис. 1). Чтобы применить алгоритм «Решето Эратосфена», нужно ввести 0 на этапе выбора количества чисел.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 1 – Вывод программы

Вывод. Таким образом, в ходе выполнения лабораторной работы, я познакомился с основами теории чисел. Изучил алгоритм Евклида, алгоритм решето Эратосфена, основную теорему арифметики, взаимно простые числа, взаимно обратные числа, модулярную арифметику, малую теорему Ферма.