Лабораторная работа 8

Вычисление наибольшего общего делителя для двух чисел при помощи алгоритма Евклида

Цель работы – используя алгоритм Эвклида создать программу, которая для чисел *a* и *b* определяет наибольший общий делитель.

Задание к работе

В программной реализации алгоритма Евклида должен быть разработан интерфейс, удобный для эксплуатации. В интерфейсе следует предусмотреть:

• ввода начальной информации из сформированного заранее файла, и файла, который создается в оболочке программы;
• ввод начальной информации с клавиатуры.

Подготовить отчет по работе. В отчете описать алгоритм Евклида, описать структуру представления данных в программе, основные функции программы, назначение функций, входные и выходные параметры функций.

Теоретический материал

Простые числа

Натуральное число *p*, больше единицы называется простым, если оно делится нацело только на единицу и на себя.

Теорема (Эвклид). Множество простых чисел бесконечно.

Обозначим через $\pi(x)$ функцию, которая равна числу простых чисел *p* в интервале $1 < x \le p$. Российский математик П.Л. Чебышев в 1850г. показал, что имеет место

$$0.921\frac{x}{\ln x} < \pi(x) < 1.106\frac{x}{\ln x}.$$

Простые числа являются важным понятием в криптографии. Многие современные криптографические системы строятся на базе простого числа. Поэтому алгоритмы генерации простых чисел и проверки на простоту сформированного числа в настоящее время являются важными инструментами при создании криптографической системы.

Заметим, что существует около 10^{151} простых чисел длиной от 1 до 512 бит включительно [5]. Для чисел, близких *n*, вероятность произвольно выбранному числу оказаться простым числом, равна (1 / ln *n*). При случайном

выборе двух простых чисел в диапазоне от 1 до 151 бита вероятность совпадения этих чисел ничтожно мала.

Пусть даны два целых числа a и b. Говорят, что число a делит b, если существует такое целое число d, что $b=ad$. Число a в этом случае называют делителем b. Для факта, что a делит b, принято обозначение $a|b$. Справедливы следующие свойства делимости:

- если $a|b$ и c – любое число, то $a|(bc)$;
- если $a|b$ и $b|c$, то $a|c$;
- если $a|b$ и $a|c$, то $a|(b \pm c)$.

Здесь уместно сделать замечание, что важную роль в арифметике целых чисел имеет теорема о делении.

Теорема о делении. Для любого целых чисел a и b, $b > 0$, существуют, и притом единственные, целые числа q и r, такие, что

$$a = bq + r,\ 0 \le r < b.$$

Определение. Натуральное число p, $p > 1$, называется составным, если число p имеет по крайней мере один положительный делитель, отличный от единицы и p.

Если число p составное, то справедлива следующая теорема.

Теорема. Для любого составного числа наименьший отличный от единицы положительный делитель является простым числом.

Одним из основных утверждений арифметики является факт, что любое натуральное число p можно единственным образом представить в виде произведения простых чисел. Например,

$$4290 = 3*2*5*11*13,$$

В общем случае каноническим разложением целого числа a называется представление в виде

$$a = p_1^{\alpha 1}\, p_2^{\alpha 2} \dots\, p_k^{\alpha k},$$

где p_i, $i = 1, 2, \dots, k$, – простые числа. Например, $133100 = 2^2 5^2 11^3$.

Заметим, что, вообще говоря, представление большого числа в канонической записи, т.е. в виде произведения простых сомножителей, является трудной и очень важной задачей в криптографии.

Определение. Общим делителем целых чисел

$$a_1, a_2, \dots, a_k$$

называется любое целое число d, такое, что

$$d|a_1,\ d|a_2,\ \ldots,\ d|a_k.$$

Определение. Наибольшим общим делителем (НОД) целых чисел a_1, a_2, …, a_k называется такой положительный общий делитель этих чисел, который делится на любой другой делитель этих чисел.

Если d – наибольший общий делитель для чисел a и b, то для него вводится обозначение $(a, b) = d$.

Теорема. Если натуральное число p не делится ни на одно простое число

$$d \le \sqrt{p},$$

то число p – простое.

Определение. Числа a_1, a_2, … a_k называются взаимно простыми, если наибольший общий делитель этих чисел равен 1.

Определение. Числа a_1, a_2, … a_k называются попарно взаимно простыми, если

$$(a_i, a_j) = 1,\ i \ne j,\ 1 \le i \le k,\ 1 \le j \le k.$$

Если числа попарно взаимно простые, то все они взаимно простые.

Пример.

Числа 15, 21, 77 – взаимно простые, но эти числа не являются попарно взаимно простыми, потому что (15, 21) = 3.

Числа 34, 53, 99, 115 – попарно взаимно простые числа.

Алгоритм Евклида

Для двух целых чисел a и b существует сравнительно быстрый метод вычисления наибольший общий делитель. Упомянутый метод вычисления наибольший общий делитель называется алгоритмом Евклида. Приведем схему работы этого алгоритма.

1. Делим число a на число b, получаем

$$a = bq_0 + r_1;$$

2. Делим число b на число r_1, имеем

$$b = r_1q_1 + r_2;$$

3. Делим число r_1 на число r_2, запишем

$$r_1 = r_2q_2 + r_3;$$

4. Делим число r_2 на число r_3, получаем

$$r_2 = r_3 q_3 + r_4;$$
$$\ldots;$$

$$r_{t-1} = r_t q_t + r_{t+1}.$$

Если остаток от деления $r_{t+1} = 0$, то в этом случае наибольший общий делитель равен числу r_t и алгоритм вычисления наибольший общий делитель завершается.

Кратко алгоритм Эвклида можно сформулировать следующим образом. Даны два целых числа a и b. Для определенности предположим, что $a > b$. Для поиска наибольшего общего делителя следует выполнить следующие операции.

1. Разделить a на b. Пусть остаток равен

$$r, 0 < r \leq a.$$

2. Если $r = 0$, то алгоритм завершается, наибольший общий делитель равен b.
3. Положим $a = b$ и $b = r$.
4. Возвращаемся на шаг 1.

Пример. Найти наибольший общий делитель чисел $a = 1173$ и $b = 323$.

1. Делим число 1173 на число 323, получаем

$$1173 = 323*3 + 204;$$

2. Делим число 323 на число 204, получаем

$$323 = 204*1 + 119;$$

3. Делим число 204 на число 119, получаем

$$204 = 119*1 + 85;$$

4. Делим число 119 на число 85, получаем

$$119 = 85*1 + 34;$$

5. Делим число 85 на число 34, получаем

$$85 = 34*2 + 17;$$

6. Делим число 34 на число 17, получаем

$$34 = 17*23 + 0;$$

Итак, в итоге получаем

$$(1173, 323) = 17.$$

Контрольные вопросы

1. Дать определение простого числа.
2. Дать определение составного числа.
3. Сформулировать алгоритм Евклида.
4. Дать определение наибольшего общего делителя.
5. Сформулировать теорему о делении двух целых чисел.