**Лабораторна робота 6**

**Обчислення найбільшого загального дільника для двох чисел за допомогою алгоритму Евкліда**

**Цель роботи** – використовуючи алгоритм Евкліда створити програму, яка для чисел а і b визначає найбільшого загального дільника.

**Завдання до роботи**

У програмній реалізації алгоритму Евкліда має бути розроблений інтерфейс, зручний для експлуатації. У інтерфейсі слід передбачити:

• введення початкової інформації з сформованого заздалегідь файлу, і файлу, який створюється в оболонці програми;

• введення початкової інформації з клавіатури.

Підготувати звіт по роботі. У звіті описати алгоритм Евкліда, описати структуру представлення даних в програмі, основні функції програми, призначення функцій, вхідні і вихідні параметри функцій.

**Теоретичний матеріал**

Прості числа Натуральне число p, більше одиниці називається простим, якщо воно ділиться без остачі лише на одиницю і на себе.

**Теорема (Евклід).** Безліч простих чисел безкінечна.

Позначимо через функцію, яка дорівнює числу простих чисел *p* в інтервалі   
. Російський математик П.Л. Чебишев в 1850г. показав, що має місце

*.*

Прості числа є важливим поняттям в криптографії. Багато сучасних криптографічних систем будуються на базі простого числа. Тому алгоритми генерації простих чисел і перевірки на простоту сформованого числа в даний час є важливими інструментами при створенні криптографічної системи.

Відмітимо, що існує близько 10151 простого числа завдовжки від 1 до 512 біт включно [5]. Для чисел, близьких n, вірогідність довільно вибраному числу виявитися простим числом, рівна (*1 / ln n*). При випадковому виборі двох простих чисел в діапазоні від 1 до 151 бита вірогідність збігу цих чисел нікчемно мала.

Хай дано два цілі числа а і b. Говорять, що число а ділить *b,* якщо існує таке ціле число *d*, що *b=ad*. Число а в цьому випадку називають дільником *b*. Для факту, що а ділить b, прийнято позначення a|b. Справедливі наступні властивості подільності*:*

• якщо *a|b і c* – будь-яке число, то *a|(bс)*;

• якщо *a|b і b|c*, то *a|c*;

• якщо *a|b і a|c*, то *a|(b ± з).*

Тут доречно зробити зауваження, що важливу роль в арифметиці цілих чисел має теорема про ділення.

**Теорема про ділення**. Для будь-якого цілих чисел *а* і *b*, *b > 0*, існують, і притому єдині, цілі числа *q* і *r*, такі, що

*.*

**Визначення.** Натуральне число *p, p > 1*, називається складеним, якщо число p має принаймні одного позитивного дільника, відмінного від одиниці і *р*. Якщо число *p* складене, то справедлива наступна теорема*.*

**Теорема.** Для будь-якого складеного числа найменший відмінний від одиниці позитивний дільник є простим числом. Одним з основних затверджень арифметики є факт, що будь-яке натуральне число *p* можна єдиним чином представити у вигляді твору простих чисел.Наприклад,

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

В загальному випадку канонічним розкладанням цілого числа а називається вистава у вигляді

,

де   
– прості числа. Наприклад, *133100 = 2252113.*

Відмітимо, що, взагалі кажучи, представлення великого числа в канонічному записі, тобто у вигляді твору простих співмножників є важкою і дуже важливим завданням в криптографії.

**Визначення.** Загальним дільником цілих чисел

називається будь-яке ціле число *d*, таке, що

.

**Визначення.** Найбільшим загальним дільником (НОД) цілих чисел   
 називається такий позитивний загальний дільник цих чиселякий ділиться на будь-якого іншого дільника цих чисел.

Якщо *d* – найбільший загальний дільник для чисел *а і b*, то для нього вводиться позначення (*а, b) = d*.

**Теорема.** Якщо натуральне число p не ділиться ні на одне просте число

*,*

тo число *p* – просте.

**Визначення.** Числа називаються взаємно простими, якщо найбільший загальний дільник цих чисел дорівнює 1.

**Визначення.** Числа називаються попарно взаємно простими, якщо

.

Якщо числа попарно взаємно прості, то всі вони взаємно прості.

**Приклад.**

Числа 15, 21, 77 – взаємно прості, але ці числа не є попарно взаємно простими, тому що (15, 21) = 3.

Числа 34, 53, 99, 115 – попарно взаємно прості числа*.*

**Алгоритм Евкліда**

Для двох цілих чисел існує порівняно швидкий метод обчислення найбільший загальний дільник. Згаданий метод обчислення найбільший загальний дільник називається алгоритмом Евкліда. Приведемо схему роботи цього алгоритму.

1. Ділимо число а на число , отримуємо

;

1. Ділимо число на число , маємо

;

1. Ділимо число на число , запишемо

;

1. Ділимо число на число , отримуємо

.

Якщо залишок від ділення , то в цьому випадку найбільший загальний дільник дорівнює числу і алгоритм обчислення найбільший загальний дільник завершується.

Коротко алгоритм Евкліда можна сформулювати таким чином. Дано два цілі числа *а і b*. Для визначеності передбачимо, що *а > b*. Для пошуку найбільшого загального дільника слід виконати наступні операції.

1. Розділити *а* на *b*. Хай залишок рівний

*.*

2. Якщо *r = 0*, то алгоритм завершується, найбільший загальний дільник рівний *b.*

3. Покладемо *а = b і b =* r.

4. Повертаємося на крок 1.

**Приклад.** Знайти найбільшого загального дільника чисел *а = 1173 і b = 323*.

1. Ділимо число *1173* на число *323,* отримуємо

*1173 = 323\*3 + 204*;

1. Ділимо число *323* на число *204*, отримуємо

*323 = 204\*1 + 119*;

1. Ділимо число *204* на число *119*, отримуємо

*204 = 119\*1 + 85*;

1. Ділимо число *119* на число *85*, отримуємо

*119 = 85\*1 + 34*;

1. Ділимо число *85* на число *34*, отримуємо

*85 = 34\*2 + 17;*

1. Ділимо число *34* на число *17,* отримуємо

*34 = 17\*23 + 0;*

Отже, у результаті отримуємо

(*1173, 323) = 17*.

**Контрольні питання**

1. Дати визначення простого числа.

2. Дати визначення складеного числа.

3. Сформулювати алгоритм Евкліда.

4. Дати визначення найбільшого загального дільника.

5. Сформулювати теорему про ділення двох цілих чисел.