**Лабораторна робота 9**

**Скласти програму вирішення рівняння виду *ax* ≡ *b mod n***

**Мета роботи:** використовуючи розширений алгоритм Евкліда, скласти

програми вирішення порівняння *ax* ≡ *b mod n*, де числа *a* і *n* взаємно прості.

**Завдання до роботи**

У програмній реалізації рішення порівняння

*ax* ≡ *bmodn*

повинен бути розроблений інтерфейс, зручний для експлуатації. В інтерфейсі слід передбачити:

* Введення початкової інформації з сформованого заздалегідь файлу і файлу, який створюється в оболонці програми;
* Введення початкової інформації з клавіатури.

Розробити тестові приклади для програми. Підготувати звіт по роботі. У звіті описати алгоритм рішення порівняння

*ax* ≡ *b mod n*,

описати структуру представлення даних в програмі, основні функції програми, призначення функцій, вхідні і вихідні параметри функцій.

**Теоретичний матеріал**

**Наприклад.** Вирішити рівняння

37*x* ≡ 5 *mod* 1940,

де *a*= 37, *b* = 5, модуль *n* = 1940.

Спочатку вирішимо рівняння

37*x* ≡ 1 mod 1940,

Тобто визначимо елемент 37-1, обернений до елемента *a* = 37. Для вирішення цього рівняння використовується розширений алгоритм Евкліда.

1. Визначаємо параметри

*U*0 = 0, *U*1 = 1, *U*2 = 1490,

*V*0 = 1, *V*1 = 0, *V*2 = 37.

1. Обчислюємо часткове *q*1 і залишок*r*2відділення модуля порівняння

*U*2 = 1940 на число *V*2 = 37. Отримуємо*q*1 = 52, а залишок*r*2 = 16. Тоді, за визначенням маємо

*t*0 = *U*0 - *V*0 × *q*1 = 0 - 1 × 52 = -52,

*U*0 = *V*0, *V*0 = *t*0,

*t*1 = *U*1 - *V*1 × *q*1 = 1 - 0 × 52 = 1,

*U*1 = *V*1, *V*1 = t1,

*t*2 = *U*3 - *V*3 × *q*1 = *r*2 = 16,

U2 = *V*2, *V*2 = *t*2.

Для другого кроку отримуємо наступні значення параметрів

*U*0 = 1, *U*1 = 0, *U*2 = 37,

*V*0 = -52, *V*1 = 1, *V*2 = 16.

1. Обчислюємо часткове *q*2 і залишок*r*3відділення модуля рівняння *U*2 = 37 на число *V*2 = 16. Отримуємо *q*2= 2, а залишок*r*3 = 5. Тоді, за визначенням

*t*0 = *U*0 - *V*0 × *q*2 = 1 - (-52) × 2 = 105,

*U*0 = *V*0, *V*0 = *t*0,

*t*1 = *U*1 - *V*1 × *q*2 = 0 - 1 × 2 = -2,

*U*1 = *V*1, *V*1 = *t*1,

*t*2 = *U*3 - *V*3 × *q*2 = *r*3 = 5,

*U*2 = *V*2, *V*2 = *t*2.

Для третього кроку отримуємо наступні значення параметрів

*U*0 = -52, *U*1 = 1, *U*2 = 16,

*V*0 = 105, V1 = -2, V2 = 5.

1. Обчислюємо часткове *q*3 і залишок *r*4 відділення модуля рівняння *U*2 = 16 на число *V*2 = 5. Отримуємо *q*3 = 3, а залишок *r*4 = 1. Тоді, за визначенням маємо

*t*0 = *U*0 – *V*0×*q*3 = -52 – (105)×3 = -367,

*U*0 = *V*0, *V*0 = *t*0,

*t*1 = *U*1 – *V*1×*q*3 = 1 – (-2)×3 = 7,

*U*1 = *V*1, *V*1 = *t*1,

*t*2 = *U*3 - *V*3 × *q*3 = *r*4 = 1,

*U*2 = *V*2, *V*2 = *t*2.

Для четвертого кроку отримуємо наступні значення параметрів

*U*0 = 105, *U*1 = -2, *U*2 = 5,

*V*0 = -367, *V*1 = 7, *V*2 = 1.

1. Обчислюємо часткове *q*4 і залишок *r*5 відділення модуля порівняння *U*2=5на число *V*2 = 1. Отримуємо *q*4 = 5, а залишок *r*5 = 0. Тоді, за визначенням маємо

*t*0 =*U*0 - *V*0 × *q*4 = 105 - (-367) × 5 = 1940,

*U*0 = *V*0, *V*0 = *t*0,

*t*1 = *U*1 - *V*1 × *q*4 = -2 - 7 × 5 = -37,

*U*1 = *V*1, *V*1 = *t*1,

*t*2 = *U*3 - *V*3 × *q*4 = *r*4 = 0,

*U*2 = *V*2, *V*2 = *t*2.

Для п'ятого кроку отримуємо наступні значення параметрів

*U*0 = -367, *U*1 = 7, *U*2 = 1,

*V*0 = 1940, *V*1 = -37, *V*2 = 0,

Алгоритм завершується тому *U*2 = 1. Рішення даного рівняння має вигляд

x ≡ 37-1*mod* 1940 ≡ (-367 +1940) *mod* 1940 ≡

≡ 1573 *mod* 1940,

тобто

*x* ≡ 1573 *mod* 1940.

Перевірка рішення рівняння 37*x* ≡ 1 *mod* 1940:

37*x* ≡ 37 × 1573 *mod* 1940 ≡ 58201 *mod* 1940 ≡

(1 + 30 × 1940) *mod* 1940 ≡ 1 *mod* 1940.

Задача рішення рівняння 37*x* ≡ 1 *mod* 1940 завершена.

Після рішення порівняння 37*x* ≡ 1 *mod*1940, можна записати рішення рівняння 37*x* ≡ 5 *mod* 1940, яке визначається формулою:

*x* = 5*x*-1*mod* 1940,

де *x-*1 є рішення рівняння 37*x*≡ 1 *mod*1940. Остаточно отримуємо,що значення  
 *x* ≡ 5*x*-1*mod* 1940 ≡ 5 × 1573 *mod* 1940 ≡ 7865 *mod* 1940 ≡ 105 *mod* 1940

є рішення рівняння 37*x* ≡ 1*mod* 1940.

**Перевірка.** Підставляємо значення *x* = 105 у рівняння 37*x* ≡ 5 *mod* 1940,

отримуємо:

37 × 105 ≡ 3885 *mod* 1940 ≡ (5 + 2 × 1940) *mod* 1940 ≡ 5 *mod* 1940,

що доводить справедливість знайденого рішення.