

# МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

## Запорізький національний технічний університет

### Методичні вказівки

до лабораторних робіт з дисципліни  
“Програмування криптоперетворень”  
для студентів спеціальностей 6.170101 "Безпека  
інформаційних і комунікаційних систем " і  
6.170102 "Системи технічного захисту інформації"  
для усіх форм навчання



2010

Методичні вказівки до лабораторних робіт з дисципліни  
“Програмування криптоперетворень” для студентів спеціальностей  
6.170101 "Безпека інформаційних і комунікаційних систем" і 6.170102  
"Системи технічного захисту інформації" для усіх форм навчання. /  
Укл.: Г.Л. Козіна. - Запоріжжя: ЗНТУ, 2010. – 34 с.

Укладачі: Г.Л.Козіна, доцент, к.ф.-м.н.

Рецензент: Л.М. Карпуков, проф, д.т.н.

Відповідальний  
за випуск: Г.Л.Козіна, доцент, к.ф.-м.н.

Затверджено  
на засіданні кафедри  
“Захист інформації”

Протокол № 6  
від “24” \_02\_ 2010 р.

## ЗМІСТ

|                                                                                                              |    |
|--------------------------------------------------------------------------------------------------------------|----|
| Лабораторна робота №1.<br>Обчислення сліду та напівсліду елемента основного поля.....                        | 4  |
| Лабораторна робота №2.<br>Програмування алгоритму розв’язання квадратного рівняння в<br>основному полі ..... | 6  |
| Лабораторна робота №3.<br>Процедура додавання точок еліптичної кривої.....                                   | 8  |
| Лабораторна робота №4.<br>Обчислення порядку точки еліптичної кривої .....                                   | 9  |
| Лабораторна робота №5.<br>Програмування алгоритму перевірки примітивності многочлена.....                    | 10 |
| Лабораторна робота №6.<br>Пошук базової точки еліптичної кривої заданого порядку .....                       | 12 |
| Література.....                                                                                              | 13 |
| Додаток А Елементи програмування криптоперетворень.....                                                      | 14 |
| Додаток Б Обчислення сліду елемента основного поля.....                                                      | 18 |
| Додаток В Обчислення напівсліду елемента основного поля.....                                                 | 19 |
| Додаток Г Розв’язання квадратного рівняння в основному полі.....                                             | 20 |
| Додаток Д Перевірка виконання умови Менезеса-Окамото-<br>Венстона.....                                       | 22 |
| Додаток Е Сума точок еліптичної кривої.....                                                                  | 23 |
| Додаток Ж Обчислення порядку точки еліптичної кривої.....                                                    | 25 |
| Додаток К Перевірка примітивності многочлена.....                                                            | 27 |
| Додаток Л Факторизація цілих чисел.....                                                                      | 30 |
| Додаток М Таблиці незвідних многочленів.....                                                                 | 31 |
| Додаток Н Рекомендовані еліптичні криви.....                                                                 | 33 |

## ЛАБОРАТОРНА РОБОТА № 1

### ОБЧИСЛЕННЯ СЛІДУ ТА НАПІВСЛІДУ ЕЛЕМЕНТА ОСНОВНОГО ПОЛЯ

**Мета роботи:** ознайомлення з основами програмування криптоперетворень, створення програмної реалізації алгоритмів обчислення сліду елементу  $x$  основного поля, обчислення напівсліду елементу  $x$  основного поля.

**Використовуване програмне забезпечення:** пакет математичних обчислень Maple.

#### 1.1 Завдання на лабораторну роботу

1. Задать розширене поле  $GF(2^m)$  по модулю незвідного многочлена  $f(t)$  (див. Додаток А).
2. Обчислити слід елемента  $x$  поля  $GF(2^m)$  (див. Додаток Б).
3. Обчислити напівслід елемента  $x$  поля  $GF(2^m)$  (див. Додаток В).

Параметри  $x$ ,  $f(t)$  взяти із таблиці згідно з номером варіанта N:

| N  | x         | f(t)        |
|----|-----------|-------------|
| 1  | 1         | $t^3+t+1$   |
| 2  | t         | $t^3+t+1$   |
| 3  | $1+t$     | $t^3+t+1$   |
| 4  | $t^2$     | $t^3+t+1$   |
| 5  | $1+t^2$   | $t^3+t+1$   |
| 6  | $t+t^2$   | $t^3+t+1$   |
| 7  | $1+t+t^2$ | $t^3+t+1$   |
| 8  | 1         | $t^3+t^2+1$ |
| 9  | t         | $t^3+t^2+1$ |
| 10 | $1+t$     | $t^3+t^2+1$ |
| 11 | $t^2$     | $t^3+t^2+1$ |
| 12 | $1+t^2$   | $t^3+t^2+1$ |
| 13 | $t+t^2$   | $t^3+t^2+1$ |
| 14 | $1+t+t^2$ | $t^3+t^2+1$ |
| 15 | 1         | $t^5+t^3+1$ |

| N  | x             | f(t)        |
|----|---------------|-------------|
| 16 | t             | $t^5+t^3+1$ |
| 17 | $1+t$         | $t^5+t^3+1$ |
| 18 | $t^2$         | $t^5+t^3+1$ |
| 19 | $1+t^2$       | $t^5+t^3+1$ |
| 20 | $t+t^2$       | $t^5+t^3+1$ |
| 21 | $1+t+t^2$     | $t^5+t^3+1$ |
| 22 | $t^3$         | $t^5+t^3+1$ |
| 23 | $1+t^3$       | $t^5+t^3+1$ |
| 24 | $t+t^3$       | $t^5+t^3+1$ |
| 25 | $1+t+t^3$     | $t^5+t^3+1$ |
| 26 | $t^2+t^3$     | $t^5+t^3+1$ |
| 27 | $1+t^2+t^3$   | $t^5+t^3+1$ |
| 28 | $1+t+t^2+t^3$ | $t^5+t^3+1$ |
| 29 | $t^4$         | $t^5+t^3+1$ |
| 30 | $1+t^4$       | $t^5+t^3+1$ |

4. Обчислити слід і напівслід елемента  $x$  поля  $GF(2^m)$ ,  $m > 160$ , по модулю примітивного многочлена  $f(t)$  (див. Додаток Л).

### **1.2 Зміст звіту**

1. Титульний лист, тема і мета роботи.
2. Результати обчислень.
3. Висновки.

### **1.3 Контрольні питання**

1. Опишіть структуру розширеного поля.
2. Що є слідом елемента розширеного поля?
3. Що є напівслідом елемента розширеного поля?
4. Які значення можуть приймати слід і напівслід елементів розширеного поля?

## ЛАБОРАТОРНА РОБОТА № 2

### ПРОГРАМУВАННЯ АЛГОРИТМУ РОЗВ'ЯЗАННЯ КВАДРАТНОГО РІВНЯННЯ В ОСНОВНОМУ ПОЛІ

**Мета роботи:** створення програмної реалізації алгоритма розв'язання квадратного рівняння  $z^2 + uz = w$  в основному полі.

**Використовуване програмне забезпечення:** пакет математичних обчислень Maple.

#### 2.1 Завдання на лабораторну роботу

Дано еліптичну криву над полем  $GF(2^m)$

$$y^2 + xy = x^3 + Ax^2 + B \bmod (f(t), 2).$$

1. Задать довільний елемент  $u$  поля  $GF(2^m)$ .
2. Обчислити  $w = u^3 + Au^2 + B \bmod (f(t), 2)$ .
3. Розв'язать квадратне рівняння  $z^2 + uz = w \bmod (f(t), 2)$  відносно змінної  $z$  (див. Додаток Г).
4. Якщо розв'язок квадратного рівняння існує, сформувати точку  $P=(u,z)$ , що належить заданій кривій.
5. Якщо квадратне рівняння не має розв'язків, оберить новий елемент поля.
6. Для знайденої точки  $P = (u,z)$  обчислити її порядок  $n$ . (Для цього виконати лабораторні роботи № 3,4.)
7. Перевірить виконання умови Менезеса-Окамото-Венстона для порядку  $n$  точки  $P$  еліптичної кривої над розширеним полем  $GF(2^m)$  (див. Додаток Д).

#### Умова Менезеса-Окамото-Венстона

Умова Менезеса-Окамото-Венстона для порядку  $n$  точки  $P$  еліптичної кривої над розширеним полем  $GF(2^m)$ :

$$2^{mk} \neq 1 \bmod n \text{ для } k=1, \mathbf{K}, 32.$$

Виконання цій умови гарантує надійність вибору параметрів еліптичної кривої і базової точки.

Параметри  $A$ ,  $B$ ,  $f(t)$  взяти із таблиці згідно з номером варіанта  $N$ :

| N  | A | B         | $f(t)$      |
|----|---|-----------|-------------|
| 1  | 1 | 1         | $t^3+t+1$   |
| 2  | 1 | $t$       | $t^3+t+1$   |
| 3  | 1 | $1+t$     | $t^3+t+1$   |
| 4  | 1 | $t^2$     | $t^3+t+1$   |
| 5  | 1 | $1+t^2$   | $t^3+t+1$   |
| 6  | 1 | $t+t^2$   | $t^3+t+1$   |
| 7  | 1 | $1+t+t^2$ | $t^3+t+1$   |
| 8  | 0 | 1         | $t^3+t+1$   |
| 9  | 0 | $t$       | $t^3+t+1$   |
| 10 | 0 | $1+t$     | $t^3+t+1$   |
| 11 | 0 | $t^2$     | $t^3+t+1$   |
| 12 | 0 | $1+t^2$   | $t^3+t+1$   |
| 13 | 0 | $t+t^2$   | $t^3+t+1$   |
| 14 | 0 | $1+t+t^2$ | $t^3+t+1$   |
| 15 | 1 | 1         | $t^5+t^3+1$ |

| N  | A | B             | $f(t)$      |
|----|---|---------------|-------------|
| 16 | 1 | $t$           | $t^5+t^3+1$ |
| 17 | 1 | $1+t$         | $t^5+t^3+1$ |
| 18 | 1 | $t^2$         | $t^5+t^3+1$ |
| 19 | 1 | $1+t^2$       | $t^5+t^3+1$ |
| 20 | 1 | $t+t^2$       | $t^5+t^3+1$ |
| 21 | 1 | $1+t+t^2$     | $t^5+t^3+1$ |
| 22 | 1 | $t^3$         | $t^5+t^3+1$ |
| 23 | 0 | $1+t^3$       | $t^5+t^3+1$ |
| 24 | 0 | $t+t^3$       | $t^5+t^3+1$ |
| 25 | 0 | $1+t+t^3$     | $t^5+t^3+1$ |
| 26 | 0 | $t^2+t^3$     | $t^5+t^3+1$ |
| 27 | 0 | $1+t^2+t^3$   | $t^5+t^3+1$ |
| 28 | 0 | $1+t+t^2+t^3$ | $t^5+t^3+1$ |
| 29 | 0 | $t^4$         | $t^5+t^3+1$ |
| 30 | 0 | $1+t^4$       | $t^5+t^3+1$ |

## 2.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Результати обчислень.
3. Висновки.

## 2.3 Контрольні питання

1. Як задається еліптична крива над розширеним полем?
2. Що є точка еліптичної кривої?
3. Як перевірити приналежність точки заданої еліптичної кривої?
4. Опишіть алгоритм розв'язання квадратного рівняння в розширеному полі.
5. Сформулюйте умову Менезеса-Окамото-Венстона для порядку точки еліптичної кривої над розширеним полем.

## ЛАБОРАТОРНА РОБОТА № 3

### ПРОЦЕДУРА ДОДАВАННЯ ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ

**Мета роботи:** створення процедури додавання точок еліптичної кривої на розширеному полі.

**Використовуване програмне забезпечення:** пакет математичних обчислень Maple.

#### 3.1 Завдання на лабораторну роботу

Дано еліптичну криву над полем  $GF(2^m)$

$$y^2 + xy = x^3 + Ax^2 + B \bmod (f(t), 2)$$

і точка  $P$ , що належить заданій кривій.

1. Перевірити приналежність точки  $P$  заданій еліптичній кривій.
2. Написати процедуру додавання точок еліптичної кривої над розширеним полем (див. Додаток Е).
3. Для точки  $P$  обчислити  $2P, 3P, 4P, \dots$

Параметри  $A, B, f(t)$  співпадають з обраними в лабораторній роботі №2, точка  $P$  є результатом виконання лабораторної роботи №2 згідно з номером варіанта  $N$ .

#### 3.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Результати обчислень.
3. Висновки.

#### 3.3 Контрольні питання

1. Як перевірити приналежність точки заданій еліптичній кривій над розширеним полем?
2. Які властивості мають точки еліптичної кривої?

## ЛАБОРАТОРНА РОБОТА № 4

### ОБЧИСЛЕННЯ ПОРЯДКУ ТОЧКИ ЕЛІПТИЧНОЇ КРИВОЇ

**Мета роботи:** створення програмної реалізації алгоритма великих-малих кроків для обчислення порядку точки еліптичної кривої.

**Використовуване програмне забезпечення:** пакет математичних обчислень Maple.

#### 4.1 Завдання на лабораторну роботу

Дано еліптичну криву над полем  $GF(2^m)$

$$y^2 + xy = x^3 + Ax^2 + B \bmod (f(t), 2)$$

і точка  $P$ , що належить заданій кривій.

1. Перевірити належність точки  $P$  заданій еліптичній кривій.
2. Знайти порядок точки  $P$  (див. Додаток Ж).

Параметри  $A$ ,  $B$ ,  $f(t)$  співпадають з обраними в лабораторній роботі №2, точка  $P$  є результатом виконання лабораторної роботи №2 згідно з номером варіанта  $N$ .

#### 4.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Результати обчислень.
3. Висновки.

#### 4.3 Контрольні питання

1. Опишіть алгоритм великих-малих кроків для обчислення порядку точки еліптичної кривої над розширеним полем.
2. Для чого необхідно знати порядок точки еліптичної кривої?
3. Якими властивостями має володіти порядок точки еліптичної кривої?

## ЛАБОРАТОРНА РОБОТА № 5

### ПРОГРАМУВАННЯ АЛГОРИТМУ ПЕРЕВІРКИ ПРИМІТИВНОСТІ МНОГОЧЛЕНА

**Мета роботи:** створення програмної реалізації алгоритма перевірки примітивності многочлена.

**Використовуване програмне забезпечення:** пакет математичних обчислень Maple.

#### 5.1 Завдання на лабораторну роботу

Дано многочлен  $f(t)$  степеня  $m$  над полем  $GF(2)$

$$f(t) = t^m + a_{m-1}t^{m-1} + \dots + a_1t + a_0,$$

де коефіцієнти многочлена  $a_i \in GF(2)$ ,  $i = 0, \dots, m-1$ .

1. Перевірити, чи є заданий многочлен примітивним (див. Додаток К).

Вибір многочлена  $f(t)$  здійснюється із таблиці за номером варіанта N:

| N  | $f(t)$                |
|----|-----------------------|
| 1  | $t^9+t^5+t^3+1$       |
| 2  | $t^9+t^5+t^3+t+1$     |
| 3  | $t^9+t^4+t^3+t^2+t+1$ |
| 4  | $t^9+t^7+t^6+1$       |
| 5  | $t^9+t^8+t^5+t+1$     |
| 6  | $t^9+t^2+t+1$         |
| 7  | $t^9+t^6+t^3+1$       |
| 8  | $t^9+t^2+1$           |
| 9  | $t^9+t^4+t+1$         |
| 10 | $t^9+t^8+t^7+1$       |
| 11 | $t^9+t^8+1$           |
| 12 | $t^9+t^5+1$           |
| 13 | $t^9+t^4+1$           |
| 14 | $t^9+t+1$             |
| 15 | $t^9+t^8+t^7+t^5+1$   |

| N  | $f(t)$                            |
|----|-----------------------------------|
| 16 | $t^9+t^8+t^7+t^5+1$               |
| 17 | $t^9+t^8+t^6+t^5+1$               |
| 18 | $t^9+t^8+t^5+t^4+1$               |
| 19 | $t^9+t^6+t^5+t^3+1$               |
| 20 | $t^9+t^7+t^4+t^3+1$               |
| 21 | $t^9+t^6+t^5+t^2+1$               |
| 22 | $t^9+t^5+t^3+t^2+1$               |
| 23 | $t^9+t^4+t^3+t+1$                 |
| 24 | $t^9+t^4+t^2+t+1$                 |
| 25 | $t^9+t^7+t^2+t+1$                 |
| 26 | $t^9+t^8+t^7+t^6+t^5+t^4+t^3+t+1$ |
| 27 | $t^9+t^6+t^5+t^4+t^3+t^2+1$       |
| 28 | $t^9+t^8+t^4+t^3+t^2+t+1$         |
| 29 | $t^9+t^6+t^4+t^3+t^2+t+1$         |
| 30 | $t^9+t^8+t^6+t^5+t^4+t^3+t^2+t+1$ |

2. Перевірьте примітивність многочлена  $f(t)$  степеня  $m$ ,  $m > 160$  (див. Додаток Л).

### 5.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Результати обчислень.
3. Висновки.

### 5.3 Контрольні питання

1. Наведіть визначення порядку елемента основного поля.
2. Що є незвідний многочлен?
3. Наведіть визначення примітивного елемента поля.
4. Що є примітивний многочлен?
5. Опишіть алгоритм перевірки примітивності многочлена.

## ЛАБОРАТОРНА РОБОТА № 6

### ПОШУК БАЗОВОЇ ТОЧКИ ЕЛІПТИЧНОЇ КРИВОЇ ЗАДАНОГО ПОРЯДКУ

**Мета роботи:** створення програмної реалізації алгоритма пошуку базової точки еліптичної кривої заданого порядку.

**Використовуване програмне забезпечення:** пакет математичних обчислень Maple.

#### 6.1 Завдання на лабораторну роботу

Дано еліптичну криву над полем  $GF(2^m)$

$$y^2 + xy = x^3 + Ax^2 + B \bmod (f(t), 2).$$

Для заданої кривої знайти базову точку заданого порядку  $n$ .  
Параметри  $A$ ,  $B$ ,  $f(t)$ ,  $n$  взяти із Додатка М.

#### 6.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Результати обчислень.
3. Висновки.

#### 6.3 Контрольні питання

1. Чому базова точка еліптичної кривої не наведено в стандарті ДСТУ 4145-2002?
2. Який діапазон степенів поля використовується в стандарті ДСТУ 4145-2002?
3. Чому дорівнює порядок базової точки?

## ЛІТЕРАТУРА

1. Фергюсон Н., Шнайер Б. Практическая криптография – М.: Диалектика, 2005. – 424 с.
2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.Ж КУДИЦ-ОБРАЗ, 2001 – 386с.
3. Topics in cryptography  
[http://en.wikipedia.org/wiki/Topics\\_in\\_cryptography](http://en.wikipedia.org/wiki/Topics_in_cryptography)
4. Нечаев В.И. Элементы криптографии (Основы теории защиты информации): Учеб. пособие для ун-тов и пед. вузов / Под ред. В.А.Садовниченко – М.: Высш.шк., 1999. – 109с.
5. Вербіцький О.В. Вступ до криптології. – Львів: ВНТЛ, 1998. – 248с.
6. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння: ДСТУ 4145: 2002. – [Чинний від 2002-03-13]. К.: Держстандарт України, 2002. – 38 с.: табл. – (Національний стандарт України).

## Додаток А

### Елементи програмування криптоперетворень

Функція **GF (2,m,f)** – створює розширене поле  $GF(2^m)$  за модулем незвідного полінома степені **m** із коефіцієнтами 0, 1.

**G163 := GF(2,163,t^163+t^7+t^6+t^3+1);**

Операція **G\_[ConvertIn](t)** конвертує елемент поля  $GF(2^m)$  у формат многочлена Maple.

**G7 := GF(2,7,t^7+t^5+t^3+t+1);**  
**f:=t^7+t^2+1;d:= G7[ConvertIn](f);**  
**G7[output](d);**  
 $f:=t^7+t^2+1 \quad d:=t+t^2+t^3+t^5 \quad 46$

Операція **G\_[input](r)** конвертує ціле число **r**,  $0 \leq r \leq 2^m-1$ , в елемент поля  $GF(2^m)$ .

Операція **G\_[output](X)** конвертує елемент **X** поля  $GF(2^m)$  в ціле число **r**,  $0 \leq r \leq 2^m-1$ .

**A:=G7[input](1);**  $A:=1$   
**xP:=G7[input](30); xP10:=G7[output](xP);**  
 $xP:=t+t^2+t^3+t^4 \quad xP10:=30$

Для перетворення десятичного числа **r** в 16-ричне використовується функція **convert (r,hex)**:

**xP16:=convert(xP10, hex);**  $1E$

Для перетворення 16-ричного числа **S** в десятичне використовується функція **convert (S,decimal, hex)**:

**r:=convert("1E", decimal, hex);**  $r:=30$

Для перетворення десятичного числа **z** в двоичне або в двоичний масив використовуються функції **convert (z, binary)** і **convert(z,base,2)** відповідно:

```
z:=19; z2:=convert(z,binary); lz2:=length(z2);
zar:=convert(z,base,2);zar[1];zar[2];zar[3]; z := 19
      z2 := 10011    lz2 := 5
zar := [1, 1, 0, 0, 1]    1      1      0
```

**Арифметичні операції над елементами поля:**

```
a:=t^2+t+1; a:= G7[ConvertIn](a);
a := t^2 + t + 1      a := 1 + t + t^2
```

```
b:=t^2;      b:= G7[ConvertIn](b);
b := t^2      b := t^2
```

```
G7[`+`](a,b);      1 + t
```

```
G7[`*`](a,b);      t^2 + t^3 + t^4
```

```
k:=3: G7[`^`](b,k); t^6
```

```
G7[`/`](a,b);      1 + t + t^3 + t^5
```

**Додаткові функції**

ceil() – округлення з надлишком

```
ceil(17/3); 6
```

floor() – округлення з недоліком

```
floor(17/3); 5
```

isprime(n) – перевірка на простоту числа n

```
isprime(15); false
```

ifactor(n) – формує прості множники числа n  
 $m := 9; m1 := 2^m - 1; pp := \text{ifactor}(m1);$   
 $m1 := 511 \quad pp := (7) (73)$

Expand() – розкриває скобки і подає добуток у вигляді многочлена

$g := t + 1; f := t + 1; h := \text{Expand}(g * f) \bmod 2;$   
 $h := t^2 + 1$

Rem(g,a,t) – повертає залишок r від ділення многочлена g на многочлен a :

$$g = a * q + r,$$

t - ім'я змінної в многочленах

$g := t^3 + 1; a := t^2 + 1; r := \text{Rem}(g, a, t) \bmod 2;$   
 $r := t + 1$

Powmod(b,n,a,t) – зведення многочлена b в степінь n за модулем многочлена a від змінної t.

$b := t; n := 5; a := t^3 + t^2 + 1;$   
 $h := \text{Powmod}(b, n, a, t) \bmod 2; \quad h := t + 1$

Gcd(a,b) – найбільший спільний дільник двох многочленів a і b .

$a := t^5 + t^3 + t + 1; b := t^2; b := b + t; \text{delt} := \text{Gcd}(a, b)$   
 $\bmod 2;$   
 $b := t^2 + t \quad \text{delt} := t + 1$

Divide(a,b,'q') перевіряє, чи ділиться многочлен a на многочлен b без залишку за модулем 2. В змінну q поміщається результат ділення у випадку успіху.

$\text{Divide}(x^3 + x^2 + 1, x + 1, 'q') \bmod 2; \quad \text{false}$   
 $\text{Divide}(x^4 + 1, x^2 + 1, 'q') \bmod 2; \quad \text{true}$   
 $q; \quad x^2 + 1$

## Процедури

Програма ілюструє роботу двох процедур – обчислення сліду елемента розширеного поля (tr2) і роботу оператора RETURN.

```

G5 := GF(2,5,t^5+t^3+1);
m:=5:
C0:=G5[input](0); C1:=G5[input](1);
xP:=G5[input](3);

C0 := 0          C1 := 1          xP := 1 + t

tr2:=proc(Px) local tx, i; tx:=Px;
for i from 1 to m-1 do
tx:=G5[``+`](G5[``^`](tx,2),Px); end do;
end proc;

tr2(xP);
1

ttt:=proc(Px) local tx,ty; tx:=G5[``*`](Px,Px);
if (tr2(Px)=C1) then ty:=C0 else ty:=C1; end if;
RETURN(tx,ty); end proc;

aa:=ttt(xP); aa[1];

aa := 1 + t2, 0
1 + t2

```

## Додаток Б

### Обчислення сліду елемента основного поля

Слідом  $tr(x)$  елемента  $x$  основного поля є значення виразу

$$tr(x) = \sum_{i=0}^{m-1} x^{2^i}.$$

Слід елемента завжди дорівнює 0 або 1 і є елементом поля  $GF(2)$ . Слід нульового елемента основного поля завжди дорівнює 0. Слід одиничного елемента основного поля дорівнює 1, тоді і тільки тоді, коли степінь основного поля  $m$  – непарне число.

#### Алгоритм обчислення сліду елемента $x$ основного поля

*Вхідні дані алгоритму:* елемент  $x$  основного поля  $GF(2^m)$ .

*Результат виконання алгоритму* – слід  $tr(x)$  елемента  $x$ .

Алгоритм обчислення сліду:

1. Приймають  $t = x$ .
2. Для  $i$  від 1 до  $m-1$  обчислюють  $t \leftarrow t^2 + x$ .
3. Результат обчислення сліду  $tr(x) = t$ .

Приклад.

Основне поле  $GF(2^5)$  з примітивним многочленом  $f(t) = t^5 + t^3 + 1$ .

$$\begin{aligned} x_1 &= t^4 + t^3 + 1, & tr(x_1) &= 1. \\ x_2 &= t^4 + t^2, & tr(x_2) &= 0. \end{aligned}$$

## Додаток В

### Обчислення напівсліду елемента основного поля

Напівслідом  $htr(x)$  елемента  $x$  основного поля непарного степеня  $m$  є елемент основного поля  $htr(x) = \sum_{i=0}^{(m-1)/2} x^{4^i}$ .

#### Алгоритм обчислення напівсліду елемента $x$ основного поля

*Вхідні дані алгоритму:* елемент  $x$  основного поля  $GF(2^m)$  непарного степеня  $m$ .

*Результат виконання алгоритму* – напівслід  $htr(x)$  елемента  $x$ .

Алгоритм обчислення сліду:

1. Приймають  $t = x$ .
2. Для  $i$  від 1 до  $\frac{m-1}{2}$  обчислюють  $t \leftarrow t^4 + x$ .
3. Результат обчислення сліду  $htr(x) = t$ .

Приклад.

Основне поле  $GF(2^5)$  з примітивним многочленом  $f(t) = t^5 + t^3 + 1$ .

$$\begin{aligned} x_1 &= t^4 + t^3 + 1, & htr(x_1) &= t^4 + t^2 + t + 1. \\ x_2 &= t^4 + t^2, & htr(x_2) &= t^2. \end{aligned}$$

## Додаток Г

### Розв'язання квадратного рівняння в основному полі

**Алгоритм розв'язання квадратного рівняння  $z^2 + uz = w$  в основному полі**

*Вхідні дані алгоритму:* квадратне рівняння  $z^2 + uz = w$ ;  $u, w \in GF(2^m)$ ;  $m$  – непарне число.

*Результат виконання алгоритму* – кількість розв'язків  $k$  квадратного рівняння й один з розв'язків цього рівняння, якщо  $k > 0$ .

Алгоритм розв'язування квадратного рівняння:

1. Якщо  $u = 0$ , то приймають  $z = w^{2^{m-1}} = \sqrt{w}$ ,  $k=1$  і переходять до кроку 8.
2. Якщо  $w = 0$ , то приймають  $z = 0$ ,  $k = 2$ , і переходять до кроку 8.
3. Обчислюють елемент основного поля  $v = wu^{-2}$ .
4. Обчислюють слід елемента  $tr(v)$ .
5. Якщо  $tr(v) = 1$ , то приймають  $k = 0$ ,  $z = 0$ , і переходять до кроку 8.
6. Обчислюють напівслід елемента  $v$ ,  $ht = htr(v)$ .
7. Обчислюють елемент основного поля  $z = ht * u$ , приймають  $k = 2$ .
8. Результат виконання алгоритму: кількість розв'язків квадратного рівняння  $k$  та один з розв'язків  $z$ , якщо  $k > 0$ .

Приклад 1.

Основне поле  $GF(2^7)$  з примітивним многочленом  $f(t) = t^7 + t^5 + t^3 + t + 1$ .

Еліптична крива

$y^2 + xy = x^3 + x^2 + B \pmod{(f(t), 2)}$ ,  $B = t+1$ , над основним полем.

Знайдемо точку еліптичної кривої.

Візьмемо випадковий елемент поля  $X = t^4 + t^3 + 1$  та обчислимо вираз  $W = X^3 + X^2 + B \bmod (f(t), 2)$  :

$$W = t^5 + t^4 + t^2 + t.$$

Для отримання другої компоненти  $Y$  точки кривої розв'яжемо квадратне рівняння

$$Y^2 + XY = W \bmod (f(t), 2).$$

Обчислимо елемент основного поля  $v = WX^{-2}$ :

$$v = t^5 + t^4 + t^2$$

та його слід  $tr(v)$  :

$$tr(v) = 0.$$

Обчислимо напівслід елемента  $v$

$$ht = htr(v) = t^5 + t^4 + t^3 + t^2.$$

Обчислимо елемент основного поля  $Y = ht * X$  :

$$Y = t^4 + t^3 + t + 1.$$

Таким чином, знайдено точка еліптичної кривої  $(X, Y) = (t^4 + t^3 + 1, t^4 + t^3 + t + 1)$ .

Приклад 2.

Візьмемо випадковий елемент поля  $X = t$  та обчислимо вираз  $W = X^3 + X^2 + B \bmod (f(t), 2)$ ,  $B = t + 1$ :

$$W = t^3 + t^2 + t + 1.$$

Розв'яжемо квадратне рівняння

$$Y^2 + XY = W \bmod (f(t), 2).$$

Обчислимо елемент основного поля  $v = WX^{-2}$ :

$$v = t^5 + t^3 + 1$$

та його слід  $tr(v)$  :

$$tr(v) = 1.$$

Оскільки  $tr(v) = 1$ , то квадратне рівняння розв'язків немає.

## Додаток Д

### Перевірка виконання умови Менезеса-Окамото-Венстона

**Алгоритм перевірки виконання умови Менезеса-Окамото-Венстона для порядку  $n$  базової точки еліптичної кривої**

*Вхідні дані алгоритму:* порядок  $n$  базової точки еліптичної кривої, визначеної над скінченним полем  $GF(2^m)$ .

*Результат виконання алгоритму* – повідомлення “умова Менезеса-Окамото-Венстона виконана” або повідомлення “умова Менезеса-Окамото-Венстона не виконана”.

*Алгоритм перевірки виконання умови Менезеса-Окамото-Венстона:*

1. Обчислюють ціле число  $s = 2^m \bmod n$ .
2. Приймають  $j = 1$ .
3. Для  $k$  від 1 до 32 виконують кроки:
  - обчислюють нове значення цілого числа  $j: j \leftarrow js \bmod n$ ;
  - якщо  $j = 1$ , то видають повідомлення “умова Менезеса-Окамото-Венстона не виконана” і припиняють виконання алгоритму.
4. видають повідомлення “умова Менезеса-Окамото-Венстона виконана”.

Приклад.

Основне поле  $GF(2^7)$  з примітивним многочленом

$$f(t) = t^7 + t^5 + t^3 + t + 1.$$

Еліптична крива

$$y^2 + xy = x^3 + x^2 + B \bmod (f(t), 2), \quad B = t+1, \text{ над основним полем.}$$

Базова точка  $P = (t^4+t^3+1, t^4+t^3+t+1)$  має порядок  $n = 67$ .

$$2^7 \bmod 67 = 61, \quad 2^{14} \bmod 67 = 36, \quad 2^{21} \bmod 67 = 52,$$

$$2^{28} \bmod 67 = 23, \quad 2^{35} \bmod 67 = 63, \quad 2^{42} \bmod 67 = 24,$$

$$2^{49} \bmod 67 = 57, \quad 2^{56} \bmod 67 = 60, \quad 2^{63} \bmod 67 = 42.$$

## Додаток Е

### Сума точок еліптичної кривої

Дано еліптична крива над розширеним полем  $GF(2^m)$

$$y^2 + xy = x^3 + Ax^2 + B \bmod (f(t), 2).$$

Сумою точок еліптичної кривої  $P = (x_P, y_P)$  и  $Q = (x_Q, y_Q)$  є нова точка кривої  $R = P + Q = (x_R, y_R)$ , координати якої визначаються формулами:

якщо  $P \neq Q$  і  $Q \neq -P$ , то

$$x_R = \lambda^2 + \lambda + x_P + x_Q + A$$

$$y_R = \lambda (x_P + x_R) + x_R + y_P$$

$$\lambda = \frac{y_P + y_Q}{x_P + x_Q}$$

якщо  $P = Q$ , то

при  $x_P = 0$   $R = 2P = \mathbf{O}$ ,

при  $x_P \neq 0$  координати точки  $R = 2P = (x_R, y_R)$  визначаються формулами

$$x_R = x_P^2 + \frac{B}{x_P^2}$$

$$y_R = x_P^2 + \left( x_P + \frac{y_P}{x_P} \right) x_R + x_R$$

Вважаємо, що  $P + (-P) = \mathbf{O}$ ,  $P + \mathbf{O} = \mathbf{O} + P$ .

Точка  $-P = (x_{-P}, y_{-P})$  називається оберненою точки  $P = (x_P, y_P)$ ,

якщо  $x_{-P} = x_P$ ,  $y_{-P} = x_P + y_P$ .

Приклад.

Дано еліптичну криву

$$y^2 + xy = x^3 + x^2 + B \bmod (f(t), 2), B = t+1,$$

над полем  $GF(2^7)$  з примітивним многочленом  $f(t) = t^7 + t^5 + t^3 + t + 1$ .

Для точки  $P = (t^4+t^3+1, t^4+t^3+t+1)$  побудуємо таблицю:

|    |                                          |
|----|------------------------------------------|
| P  | $(t^4+t^3+1, t^4+t^3+t+1)$               |
| 2P | $(t^5+t^4+t^3+t+1, t^6+t^5+t^3+t^2+t+1)$ |
| 3P | $(t^6+t^4+t^2+1, t^6+t^5+t^3+1)$         |
| 4P | $(t^5+t^3+1, t^5+t^4+t^2+t+1)$           |
| 5P | $(t^5+t^4+t^3+t^2+t+1, t^5+t^2+1)$       |
| 6P | $(t^6+t^5+t^4+t+1, t^5+t^3+t)$           |
| 7P | $(t^6+t^5+t^3+t^2+t+1, t^5+t^4+1)$       |
| 8P | $(t^5+t^3+t^2+t+1, t^6+t^5+t^4+t+1)$     |
| 9P | $(t^3+1, t^6+t^4+t^3+t)$                 |
| 10 | $(t^6+t^5+t^4+t^3+1, t^4+t^3+1)$         |
| 11 | $(t^5+1, t^3)$                           |
| 12 | $(t^4+t^3+t+1, t^5+t^4+t^2+t+1)$         |

## Додаток Ж

### Обчислення порядку точки еліптичної кривої

Дано еліптична крива над розширеним полем  $GF(2^m)$

$$y^2 + xy = x^3 + Ax^2 + B \bmod (f(t), 2)$$

і точка  $P$ , яка належить заданій кривій. Знайдемо порядок точки  $P$ .

Для цього необхідно розв'язати порівняння відносно  $z$   
 $z \cdot P = \mathbf{O}$ .

#### Алгоритм обчислення порядку точки еліптичної кривої

Застосуємо алгоритм великих-малих кроків.

Нехай  $n$  - максимальна оцінка порядку групи точок еліптичної кривої, яка може бути отримана по теоремі Хасе  
 $(q+1-2\sqrt{q} \leq n \leq q+1+2\sqrt{q}, q=2^m)$ ,  $P$  - точка еліптичної кривої.

Обчислимо  $k := \lceil \sqrt{n} \rceil$ , де  $\lceil a \rceil$  - округлення з надлишком.

1. Будуємо таблицю пар  $(j, jP)$  для  $j = 1, 2, \dots, k$ .
2. Обчислимо  $\alpha := -kP$ .
3.  $\gamma := \mathbf{O}$ .
4. Для  $i$  від 0 до  $k-1$   
 перевіряємо, чи є  $\gamma$  другою компонентою у таблиці  
 якщо  $\gamma = jP$ , то вважаємо  $z = k \cdot i + j$   
 $\gamma := \gamma + \alpha$ .

Приклад.

Дано еліптичну криву

$$y^2 + xy = x^3 + x^2 + B \bmod (f(t), 2), B = t+1,$$

над полем  $GF(2^7)$  з примітивним многочленом  $f(t) = t^7 + t^5 + t^3 + t + 1$ .

По теоремі Хасе максимальна оцінка порядку групи точок кривої дорівнює  $n = 2^7 + 1 + 2\sqrt{2^7} = 128 + 1 + 22.63 = 151$ . Звідси  $k = 13$ .

Знайдемо порядок точки  $P = (t^4 + t^3 + 1, t^4 + t^3 + t + 1)$  за допомогою алгоритму великих-малих кроків.

Побудуємо таблицю:

|    |                                          |
|----|------------------------------------------|
| P  | $(t^4+t^3+1, t^4+t^3+t+1)$               |
| 2P | $(t^5+t^4+t^3+t+1, t^6+t^5+t^3+t^2+t+1)$ |
| 3P | $(t^6+t^4+t^2+1, t^6+t^5+t^3+1)$         |
| 4P | $(t^5+t^3+1, t^5+t^4+t^2+t+1)$           |
| 5P | $(t^5+t^4+t^3+t^2+t+1, t^5+t^2+1)$       |
| 6P | $(t^6+t^5+t^4+t+1, t^5+t^3+t)$           |
| 7P | $(t^6+t^5+t^3+t^2+t+1, t^5+t^4+1)$       |
| 8P | $(t^5+t^3+t^2+t+1, t^6+t^5+t^4+t+1)$     |
| 9P | $(t^3+1, t^6+t^4+t^3+t)$                 |
| 10 | $(t^6+t^5+t^4+t^3+1, t^4+t^3+1)$         |
| 11 | $(t^5+1, t^3)$                           |
| 12 | $(t^4+t^3+t+1, t^5+t^4+t^2+t+1)$         |
| 13 | $(t^6+t^4+t^2+t+1, t^6+t^4)$             |

Знайдемо  $\alpha := -k P = -13 P = (t^6+t^4+t^2+t+1, t^2+t+1) \Rightarrow$

$$\alpha = (t^6+t^4+t^2+t+1, t^2+t+1).$$

$$\gamma := \mathbf{O}.$$

$$i = 0 \quad \gamma := \gamma + \alpha = \mathbf{O} + (t^6+t^4+t^2+t+1, t^2+t+1) = (t^6+t^4+t^2+t+1, t^2+t+1).$$

$$\begin{aligned} i = 1 \quad \gamma &= \gamma + \alpha = (t^6+t^4+t^2+t+1, t^2+t+1) + (t^6+t^4+t^2+t+1, t^2+t+1) = \\ &= (t+1, t^6+t^3+1). \end{aligned}$$

$$\begin{aligned} i = 2 \quad \gamma &= \gamma + \alpha = (t+1, t^6+t^3+1) + (t^6+t^4+t^2+t+1, t^2+t+1) = \\ &= (t^6+t^4+1, t^5+t^4+t^3). \end{aligned}$$

$$\begin{aligned} i = 3 \quad \gamma &= \gamma + \alpha = (t^6+t^4+1, t^5+t^4+t^3) + (t^6+t^4+t^2+t+1, t^2+t+1) = \\ &= (t^6+t^5+t+1, t^6+t^3+t+1). \end{aligned}$$

$$\begin{aligned} i = 4 \quad \gamma &= \gamma + \alpha = (t^6+t^5+t+1, t^6+t^3+t+1) + (t^6+t^4+t^2+t+1, t^2+t+1) = \\ &= (t^5+t^4+t^3+t+1, t^6+t^5+t^3+t^2+t+1). \end{aligned}$$

$$i = 5 \quad j = 2 \quad \Rightarrow z = k \cdot i + j = 13 \cdot 5 + 2 = 67.$$

Порядок точки  $P = (t^4+t^3+1, t^4+t^3+t+1)$  дорівнює 67.

## Додаток К

### Перевірка примітивності многочлена

Многочлен  $f(t)$  степеня  $m$  над полем  $GF(2)$  має вигляд

$$f(t) = t^m + a_{m-1}t^{m-1} + \dots + a_1t + a_0,$$

де коефіцієнти многочлена  $a_i \in GF(2)$ ,  $i = 0, 1, \dots, m-1$ .

Порядок елемента  $u \neq 0$  основного поля  $GF(2^m)$  по модулю многочлена  $f(t)$  є найменше натуральне число  $k$ , таке що  $u^k = 1 \pmod{f(t)}$ .

Примітивний елемент основного поля є елемент основного поля  $GF(2^m)$ , порядок якого дорівнює  $2^m - 1$ , тобто примітивний елемент є генератором мультиплікативної групи поля.

Незвідний многочлен над полем  $GF(2)$  є многочлен ненульового степеня, що ділиться над полем  $GF(2)$  без залишку тільки на самого себе і многочлени нульового степеня.

Незвідний многочлен  $f(t)$  є примітивним, якщо елемент  $t$  основного поля  $GF(2^m)$  по модулю многочлена  $f(t)$  має порядок  $2^m - 1$ . (Тобто елемент  $t$  є примітивним елементом поля  $GF(2^m)$  по модулю многочлена  $f(t)$ .)

Приклади.

Многочлен  $f(t) = t^3 + t^2 + 1$  степеня 3 є примітивним, оскільки він незвідний та  $2^3 - 1 = 7$  є просте число і будь-який елемент поля  $GF(2^3)$  є примітивним елементом.

Многочлен  $f(t) = t^9 + t^4 + t^2 + t + 1$  степеня 9 є незвідним, або не є примітивним, оскільки  $2^9 - 1 = 511 = 7 \cdot 73$  і  $t^{73} \pmod{f(t)} = 1$ , тобто елемент  $t$  породжує тільки підгрупу порядку 73 мультиплікативної групи поля  $GF(2^9)$ .

Якщо  $2^m - 1$  є просте число, то будь-який незвідний многочлен степеня  $m$  є примітивним.

**Алгоритм перевірки примітивності многочлена  $f(t)$  степеня  $m$  над скінченним полем  $GF(2)$**

*Вхідні дані алгоритму:* многочлен  $f(t) = t^m + a_{m-1}t^{m-1} + \mathbf{L} + a_0$ , коефіцієнти якого належать до поля  $GF(2)$ ,  $m$  – непарне число.

*Результат виконання алгоритму* – повідомлення “многочлен примітивний” або повідомлення “многочлен не примітивний”.

Алгоритм перевірки примітивності многочлена:

1. Приймають  $g(t) = t$ .

2. Для  $i$  від 1 до  $\left\lfloor \frac{m}{2} \right\rfloor$  виконують кроки:

– обчислюють многочлен  $g(t) \leftarrow g(t)^2 \bmod f(t)$ .

– обчислюють найбільший спільний дільник  $d(t)$  многочленів  $f(t)$  і  $g(t) + t$ .

– якщо  $d(t) \neq 1$ , то видають повідомлення “многочлен не примітивний” і припиняють виконання алгоритму.

3. За допомогою факторизації (див. Додаток Л) визначають прості дільники  $p_1, \mathbf{L}, p_k$  числа  $2^m - 1$ .

4. Для  $i$  від 1 до  $k$  виконують кроки 4.1 і 4.2:

– обчислюють многочлен  $d_i(t) = t^{\frac{2^m-1}{p_i}} \bmod f(t)$ .

– якщо  $d_i(t) = 1$ , то видають повідомлення “многочлен не примітивний” і припиняють виконання алгоритму.

5. видають повідомлення “многочлен примітивний”.

**Приклад 1.**

Перевіримо примітивності многочлена  $f(t) = t^3 + t^2 + 1$  степеня 3.

$$m = 3, \left\lfloor \frac{m}{2} \right\rfloor = 1.$$

Положимо  $g(t) = t$  і обчислимо  $g(t) = t^2 \bmod f(t)$ .

Знайдемо найбільший спільний дільник  $d(t)$  многочленів  $f(t)$  і  $g(t)+t$  :

$$d(t) = \text{НСД}(t^3 + t^2 + 1, t^2 + t) = 1.$$

Визначимо дільники числа  $2^m - 1 = 7$ . Звідси

$$p_1 = 7 \text{ і } d_1(t) = t^1 \bmod f(t) = t.$$

Оскільки  $d_1(t) \neq 1$ , то многочлен  $f(t) = t^3 + t^2 + 1$  є примітивним.

Приклад 2.

Перевіримо примітивності многочлена степеня 9

$$f(t) = t^9 + t^6 + t^4 + t^3 + t^2 + t + 1.$$

$$m = 9, \left\lfloor \frac{m}{2} \right\rfloor = 4.$$

Положимо  $g(t) = t$ .

$$i = 1: g(t) = t^2, d(t) = \text{НСД}(t^9 + t^6 + t^4 + t^3 + t^2 + t + 1, t^2 + t) = 1.$$

$$i = 2: g(t) = t^4, d(t) = \text{НСД}(t^9 + t^6 + t^4 + t^3 + t^2 + t + 1, t^4 + t) = 1.$$

$$i = 3: g(t) = t^8, d(t) = \text{НСД}(t^9 + t^6 + t^4 + t^3 + t^2 + t + 1, t^8 + t) = 1.$$

$$i = 4: g(t) = t^{16}, d(t) = \text{НСД}(t^9 + t^6 + t^4 + t^3 + t^2 + t + 1, t^{16} + t) = 1.$$

Визначимо дільники числа  $2^m - 1 = 511$ . Звідси

$$p_1 = 7 \text{ і } p_2 = 73$$

$$d_1(t) = t^{73} \bmod f(t) = t^8 + t^5 + t^2$$

$$d_2(t) = t^7 \bmod f(t) = t^7$$

Оскільки  $d_i(t) \neq 1$ , то многочлен  $f(t) = t^3 + t^2 + 1$  є примітивним.

## Додаток Л

### Факторізація цілих чисел

Процес розкладання числа на множники називається факторізацією.

Алгоритм р- Полларда знаходить дільник заданого цілого числа  $n$ .

#### Алгоритм г- Полларда факторізації цілих чисел

1. Перевіряємо, чи є число  $n$  простим.
2. Якщо  $n$  - складне число, виконуємо:  
 $a:=2$   $b:=2$   
цикл по  $i$   
 $a := (a^2 + 1) \bmod n$  ;  $b := (b^2 + 1) \bmod n$  ;  $b:=(b^2 + 1) \bmod n$  ;  
 $d := \text{НСД}(a - b, n)$  ;  
Якщо  $d > 1$ , повертаємо «  $d$  - дільник числа  $n$  ».

Приклад.

Знайдіть всі прості множники числа  $n = 2^{11}-1 = 2047$ .

За допомогою тесту на простоту перевіряємо, чи є число  $n=2047$  простим.

Число  $n = 2047$  є складним, тобто має множників.

Застосовуємо алгоритм р- Полларда:

$a:=2$ ;  $b:=2$ ;

$i:=1$      $a:=5$ ;     $b:=5$ ;     $b:=26$ ;     $\text{НСД}(5-26, 2047)=1$

$i:=2$      $a:=26$ ;     $b:=677$ ;  $b:=1849$ ;  $\text{НСД}(26-1849, 2047)=1$

$i:=3$      $a:=677$ ;     $b:=312$ ;  $b:=1136$ ;  $\text{НСД}(677-1136, 2047)=1$

$i:=4$      $a:=1849$ ;  $b:=887$ ;  $b:=722$ ;     $\text{НСД}(1849-722, 2047)=23$

Знайдено дільник 23 числа 2047.

Дільник 23 є просте число.

Другий дільник  $2047/23 = 89$  також є просте число.

**Додаток М**  
**Таблиці незвідних многочленів**

**Таблиця М.1 – Незвідні многочлени степені 1–3–5–7**

|                             |                             |                                         |
|-----------------------------|-----------------------------|-----------------------------------------|
| $x + 1$                     | $x^7 + x^6 + 1$             | $x^7 + x^5 + x^4 + x^3 + 1$             |
| $x^3 + x + 1$               | $x^7 + x^4 + 1$             | $x^7 + x^5 + x^3 + x + 1$               |
| $x^3 + x^2 + 1$             | $x^7 + x^3 + 1$             | $x^7 + x^5 + x^2 + x + 1$               |
| $x^5 + x^3 + 1$             | $x^7 + x + 1$               | $x^7 + x^4 + x^3 + x^2 + 1$             |
| $x^5 + x^2 + 1$             |                             |                                         |
| $x^5 + x^4 + x^3 + x^2 + 1$ | $x^7 + x^6 + x^5 + x^4 + 1$ | $x^7 + x^3 + x^2 + x + 1$               |
| $x^5 + x^4 + x^2 + x + 1$   | $x^7 + x^6 + x^5 + x^2 + 1$ | $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$ |
| $x^5 + x^4 + x^3 + x + 1$   |                             | $x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$   |
| $x^5 + x^3 + x^2 + x + 1$   | $x^7 + x^6 + x^4 + x + 1$   | $x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$   |
|                             | $x^7 + x^6 + x^3 + x + 1$   | $x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$   |

Таблиця М.2 - Рекомендовані примітивні многочлени

| №<br>ч/ч | Степінь<br>поля $m$ | Примітивний<br>многочлен   | №<br>ч/ч | Степінь<br>поля $m$ | Примітивний<br>многочлен    |
|----------|---------------------|----------------------------|----------|---------------------|-----------------------------|
| 1        | 163                 | $x^{163}+x^7+x^6+x^3+1$    | 31       | 337                 | $x^{337}+x^{10}+x^6+x+1$    |
| 2        | 167                 | $x^{167}+x^6+1$            | 32       | 347                 | $x^{347}+x^{17}+x^6+x+1$    |
| 3        | 173                 | $x^{173}+x^{10}+x^2+x+1$   | 33       | 349                 | $x^{349}+x^6+x^5+x^2+1$     |
| 4        | 179                 | $x^{179}+x^4+x^2+x+1$      | 34       | 353                 | $x^{353}+x^{26}+x^7+x^3+1$  |
| 5        | 181                 | $x^{181}+x^7+x^6+x+1$      | 35       | 359                 | $x^{359}+x^{18}+x^4+x^2+1$  |
| 6        | 191                 | $x^{191}+x^9+1$            | 36       | 367                 | $x^{367}+x^{21}+1$          |
| 7        | 193                 | $x^{193}+x^{15}+1$         | 37       | 373                 | $x^{373}+x^9+x^6+x+1$       |
| 8        | 197                 | $x^{197}+x^{21}+x^2+x+1$   | 38       | 379                 | $x^{379}+x^{17}+x^6+x+1$    |
| 9        | 199                 | $x^{199}+x^{11}+x^2+x+1$   | 39       | 383                 | $x^{383}+x^9+x^5+x+1$       |
| 10       | 211                 | $x^{211}+x^{12}+x^6+x+1$   | 40       | 389                 | $x^{389}+x^{17}+x^{10}+x+1$ |
| 11       | 223                 | $x^{223}+x^{12}+x^2+x+1$   | 41       | 397                 | $x^{397}+x^{22}+x^3+x+1$    |
| 12       | 227                 | $x^{227}+x^{21}+x^2+x+1$   | 42       | 401                 | $x^{401}+x^{29}+x^4+x+1$    |
| 13       | 229                 | $x^{229}+x^{21}+x^2+x+1$   | 43       | 409                 | $x^{409}+x^{15}+x^6+x+1$    |
| 14       | 233                 | $x^{233}+x^9+x^4+x+1$      | 44       | 419                 | $x^{419}+x^{21}+x^{14}+x+1$ |
| 15       | 239                 | $x^{239}+x^{15}+x^2+x+1$   | 45       | 421                 | $x^{421}+x^7+x^4+x+1$       |
| 16       | 241                 | $x^{241}+x^{15}+x^4+x+1$   | 46       | 431                 | $x^{431}+x^5+x^3+x+1$       |
| 17       | 251                 | $x^{251}+x^{14}+x^4+x+1$   | 47       | 433                 | $x^{433}+x^{15}+x^5+x+1$    |
| 18       | 257                 | $x^{257}+x^{12}+1$         | 48       | 439                 | $x^{439}+x^8+x^3+x^2+1$     |
| 19       | 263                 | $x^{263}+x^{27}+x^2+x+1$   | 49       | 443                 | $x^{443}+x^{28}+x^3+x+1$    |
| 20       | 269                 | $x^{269}+x^7+x^6+x+1$      | 50       | 449                 | $x^{449}+x^{25}+x^5+x^3+1$  |
| 21       | 271                 | $x^{271}+x^{16}+x^3+x+1$   | 51       | 457                 | $x^{457}+x^{16}+1$          |
| 22       | 277                 | $x^{277}+x^{23}+x^3+x^2+1$ | 52       | 461                 | $x^{461}+x^{23}+x^4+x+1$    |
| 23       | 281                 | $x^{281}+x^9+x^4+x+1$      | 53       | 463                 | $x^{463}+x^{24}+x^3+x+1$    |
| 24       | 283                 | $x^{283}+x^{26}+x^9+x+1$   | 54       | 467                 | $x^{467}+x^{28}+x^3+x+1$    |
| 25       | 293                 | $x^{293}+x^{11}+x^6+x+1$   | 55       | 479                 | $x^{479}+x^{25}+x^6+x+1$    |
| 26       | 307                 | $x^{307}+x^8+x^4+x^2+1$    | 56       | 487                 | $x^{487}+x^{15}+x^2+x+1$    |
| 27       | 311                 | $x^{311}+x^{29}+x^4+x+1$   | 57       | 491                 | $x^{491}+x^{17}+x^6+x^2+1$  |
| 28       | 313                 | $x^{313}+x^7+x^3+x+1$      | 58       | 499                 | $x^{499}+x^{29}+x^6+x^2+1$  |
| 29       | 317                 | $x^{317}+x^9+x^5+x^2+1$    | 59       | 503                 | $x^{503}+x^3+1$             |
| 30       | 331                 | $x^{331}+x^{12}+x^5+x^2+1$ | 60       | 509                 | $x^{509}+x^{23}+x^3+x^2+1$  |

## Додаток Н

### Рекомендовані еліптичні криві

**Таблиця Н.1** - Рекомендовані еліптичні криві над полем  $GF(2^m)$

| m   | Еліптична крива $y^2 + xy = x^3 + Ax^2 + B$                                                                                                                                                                               |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 163 | A=1<br>B=5FF6108462A2DC8210AB403925E638A19C1455D21<br>n=400000000000000000002BEC12BE2262D39BCF14D                                                                                                                         |
| 167 | A=1<br>B=6EE3CEEB230811759F20518A0930F1A4315A827DAC<br>n=3FFFFFFFFFFFFFFFFFFFFFFFFB12EBCC7D7F29FF7701F                                                                                                                    |
| 173 | A=0<br>B=108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9<br>n=8000000000000000000000189B4E67606E3825BB2831                                                                                                                   |
| 179 | A=1<br>B=4A6E0856526436F2F88DD07A341E32D04184572BEB710<br>n=3FFFFFFFFFFFFFFFFFFFFFFFFB981960435FE5AB64236EF                                                                                                               |
| 191 | A=1<br>B=7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03<br>n=400000000000000000000000069A779CAC1DABC6788F7474F                                                                                                          |
| 233 | A=1<br>B=06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA/<br>936ECE454D2C<br>n=1000000000000000000000000000000000000000000013E974E72F8A6922031D260/<br>3CFE0D7                                                            |
| 257 | A=0<br>B=1CEF494720115657E18F938D7A7942394FF9425C1458C5786/<br>1F9EEA6ADBE3BE10<br>n= 800000000000000000000000000000000000000000006759213AF182E987D3E/<br>17714907D470D                                                   |
| 307 | A=1<br>B=393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E24/<br>1050DF18B6090BDC90186904968BB<br>n=3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC079C2F38/<br>25DA70D390FBBA588D4604022B7B7                                     |
| 367 | A=1<br>B=43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64/<br>B0C2AFE42CADAB8F93D92394C79A79755437B56995136<br>n=4000000000000000000000000000000000000000000000000000009C300B7/<br>5A3FA824F22428FD28CE8812245EF44049B2D49 |

|     |                                                                                                                                                                                                                                                                 |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 431 | A=1<br>B=03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF98/<br>8D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117/<br>DAA469C640CAF3<br>n=3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF/<br>FFFFFFFFBA3175458009A8C0A724F02F81AA8A1FCBAF80D90/<br>C7A95110504CF |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Зображення коефіцієнта  $B$  відповідає рекомендованому примітивному многочлену із Додатка М. Символ “/” означає, що написання коефіцієнта  $B$  еліптичної кривої або її порядку  $n$  розділено на рядки.