Кафедра захисту інформації НУ “ЗП”

Особливості використання ізогеній еліптичних кривих в криптографічних протоколах

Виконав студент групи РТ-810м:
Пономаренко Є.О.
Науковий керівник:
проф.Неласа Г.В.

2021 рік

МЕТА І ЗАДАЧІ

Мета:

Ознайомлення з методами обчислення ізогеній на суперсингулярних еліптичних кривих за допомогою загальної схеми алгоритму Вєлу, які дозволяють побудувати постквантові криптографічні протоколи.

Задачі:

- проведення дослідження суперсингулярних еліптичних кривих
- реалізація обчислювального прикладу за допомогою загальної схеми алгоритму Вєлу.
- ознайомлення з відповідним протоколом розділення ключа Діффі-Хеллмана.

- Еліптичні криві – одні з найперспективніших інструментів для побудови криптографічних алгоритмів.
- Криптосистеми, засновані на обчисленні алгебраїчних відображень, ізогеній, еліптичних кривих, надаються стійкими по відношенню до квантового комп'ютера.
- Термін "ізогенія" був введений Андре Вейлем.

МАТЕМАТИЧНИЙ АПАРАТ РОБОТИ З ІЗОГЕНІЯМИ НА ЕЛІПТИЧНИХ КРИВИХ

- У математиці ізогенія – це морфізм алгебраїчних груп, який є сюр'єктивним і має скінчене ядро.
- Тобто:

відображення $f: X \to Y$ є сюр'єктивним, якщо для кожного y з множини Y, існує щонайменш один x з множини X такий, що $f(x) = y$.

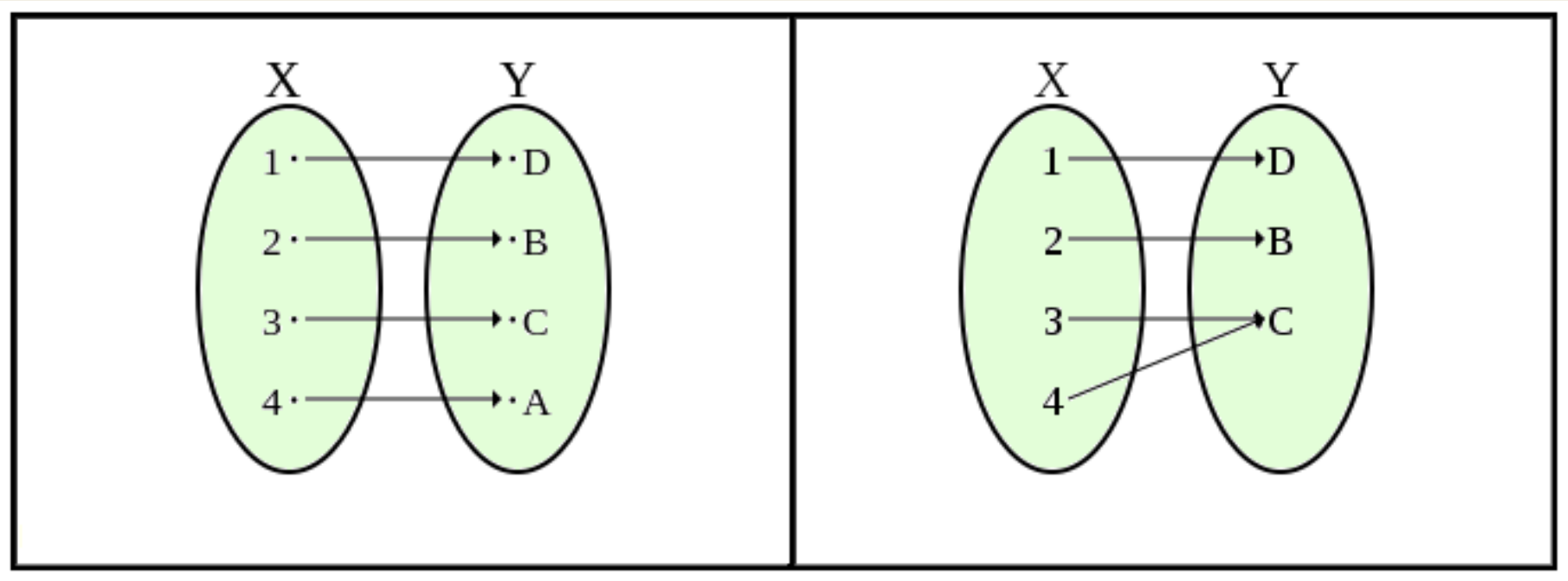


Рисунок – Сюр'єктивне відображення

- У криптографії ізогенія – це раціональне відображення $\varphi: E_1 \to E_2$, де E_1 та E_2 є еліптичними кривими, а $\varphi(P_\infty) = P_\infty$.
- Ядром ізогенії є множина точок кривої E_1 , відображеної в $P_\infty \in E_2$.
- Для ізогенії φ існує дуальна ізогенія $\hat{\varphi}: E_2 \to E_1$ така, що $\hat{\varphi}\varphi = [l]$, де l – множення точки кривої E_1 на число l.
- Аналогічно $\varphi\hat{\varphi} = [l]$, де l – множення точки кривої E_2 на число l.

- Ізогенію можна виразити за допомогою раціональної функції: точка (x, y) відображається в точку з координатами $\left(\frac{f1(x,y)}{f2(x,y)}, \frac{g1(x,y)}{g2(x,y)}\right)$, де f_1, f_2, g_1, g_2 - поліноми.
- Якщо існує такого роду відображення між двома кривими, то вони називаються ізогенними.
- Теорема Джона Торренса Тейта: дві криві над одним кінцевим полем ізогенні тоді і тільки тоді, коли порядки їх груп рівні.

АЛГОРИТМ ВЄЛУ

Крива $El: y^2 = x^3 + Ax + B$,
одна з її підгруп C

1. Відкидаємо точку на нескінченності.
2. Знаходимо C_2- безліч точок парного порядку з C .
R - решта усіх.
3. Розбиваємо R на дві частини -R_+ і R_-:
якщо точка P – в R_+, то зворотна їй – в R_-.
4. Множина $S = C_2 \cup R_+$

Для кожної точки $Q = (x_Q, y_Q)$ з S

$g_Q^x = 3x_Q^2 + A$

$g_Q^y = -2y_Q$

$if(Q = -Q)$

$v_Q = g_Q^x$

$else$

$v_Q = 2g_Q^x$

$u_Q = (g_Q^y)^2$

$v = \sum_{Q \in S} (v_Q)$

$w = \sum_{Q \in S} (u_Q + x_Q v_Q)$

$A' = A - 5v$

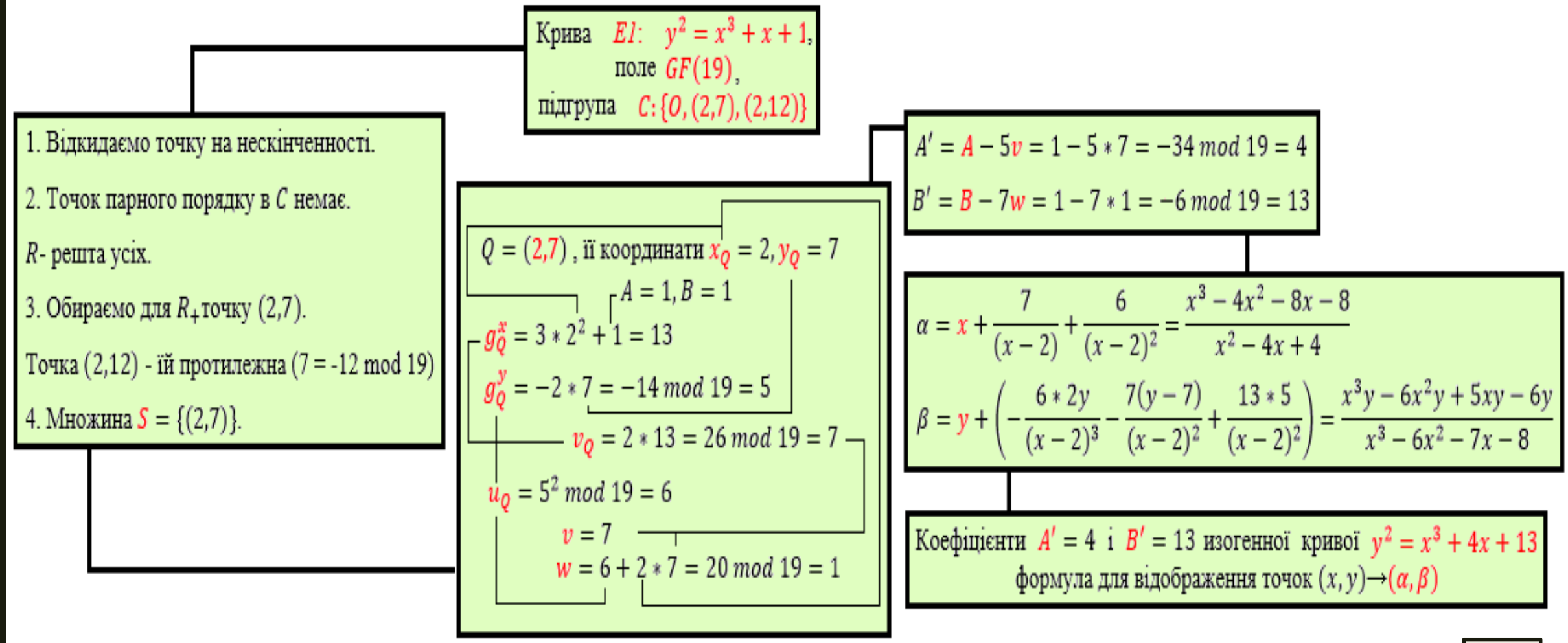
$B' = B - 7w$

$$\alpha = x + \sum_{Q \in S} \left(\frac{v_Q}{(x - x_Q)} + \frac{u_Q}{(x - x_Q)^2} \right)$$

$$\beta = y + \sum_{Q \in S} \left(-\frac{u_Q 2y}{(x - x_Q)^3} - \frac{v_Q (y - y_Q)}{(x - x_Q)^2} + \frac{g_Q^x g_Q^y}{(x - x_Q)^2} \right)$$

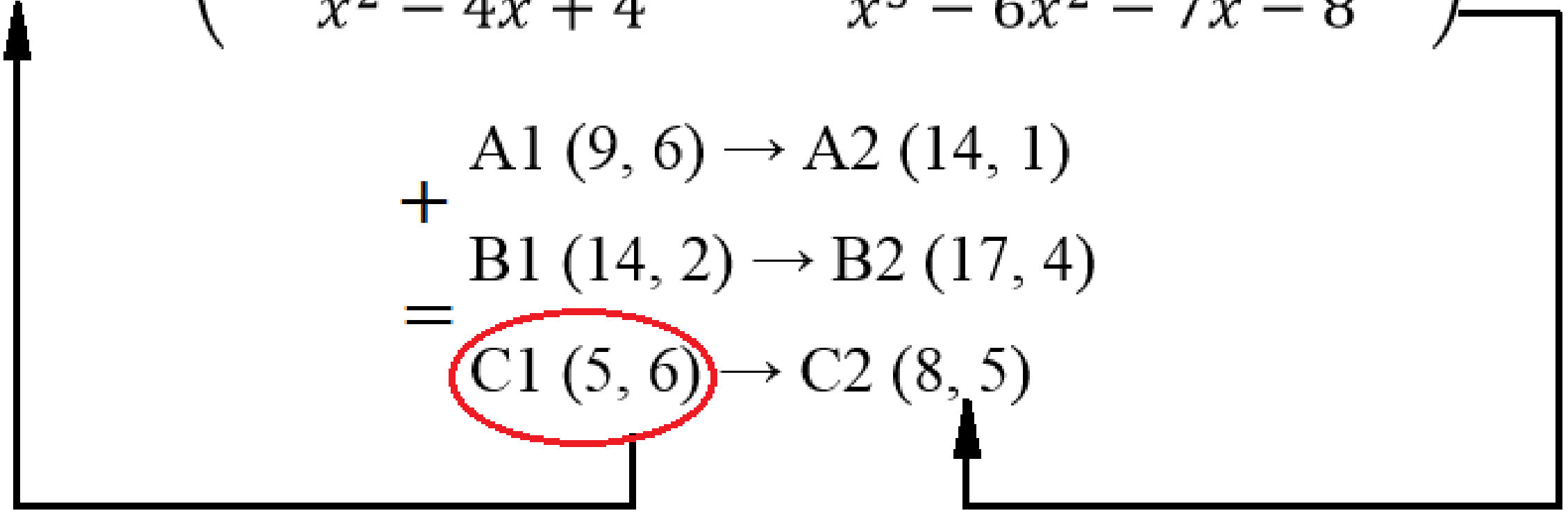
Коефіцієнти A' і B' изогенної кривої
формула для відображення точок $(x, y) \rightarrow (\alpha, \beta)$

ПРИКЛАД ФОРМУВАННЯ ІЗОГЕНІЙ НА ЕЛІПТИЧНИХ КРИВИХ



ПЕРЕВІРКА СФОРМОВАНОГО РАЦІОНАЛЬНОГО ВІДОБРАЖЕННЯ

$$(x, y) \rightarrow \left(\frac{x^3 - 4x^2 - 8x - 8}{x^2 - 4x + 4}, \frac{x^3y - 6x^2y + 5xy - 6y}{x^3 - 6x^2 - 7x - 8} \right)$$



РОЗРАХУНКОВИЙ ПРИКЛАД У СПЕЦІАЛІЗОВАНОМУ СЕРЕДОВИЩІ

```
> msolve(y^2=x^3+x+1,19);
```

$\{x = 5, y = 6\}, \{x = 5, y = 13\}, \{x = 7, y = 3\}, \{x = 7, y = 16\}, \{x = 0, y = 1\}, \{x = 0, y = 18\},$
$\{x = 2, y = 7\}, \{x = 2, y = 12\}, \{y = 13, x = 9\}, \{y = 6, x = 9\}, \{y = 2, x = 10\}, \{x = 10, y = 17\},$
$\{x = 13, y = 8\}, \{x = 13, y = 11\}, \{y = 2, x = 14\}, \{y = 17, x = 14\}, \{y = 3, x = 15\},$
$\{y = 16, x = 15\}, \{y = 3, x = 16\}, \{y = 16, x = 16\}$

```
> msolve(y^2=x^3+4*x+13,19);
```

$\{x = 11, y = 1\}, \{x = 11, y = 18\}, \{x = 8, y = 14\}, \{x = 8, y = 5\}, \{x = 17, y = 15\}, \{x = 17, y = 4\},$
$\{y = 18, x = 13\}, \{y = 1, x = 13\}, \{y = 1, x = 14\}, \{y = 18, x = 14\}, \{y = 3, x = 15\},$
$\{y = 16, x = 15\}, \{x = 4, y = 13\}, \{x = 4, y = 6\}, \{y = 5, x = 5\}, \{y = 14, x = 5\}, \{y = 5, x = 6\},$
$\{y = 14, x = 6\}, \{x = 7, y = 2\}, \{x = 7, y = 17\}$

Алгоритм Вєлу

```
A:=1;B:=1;Q:=(2,7);  n:=19;
```

$A := 1$

$B := 1$

$Q := 2, 7$

$n := 19$

```
xq:=2;  yq:=7;
```

$xq := 2$

$yq := 7$

```
gx:=3*xq^2+A mod n;  gy:=-2*yq mod n;
```

$gx := 13$

$gy := 5$

```
uq:=(gy)^2 mod n;
```

$uq := 6$

```
v:=vq mod n;
```

$v := 7$

```
w:=uq+xq*vq mod n;
```

$w := 1$

```
AA:=A-5*v mod n;
BB:=B-7*w mod n;
```

$AA := 4$

$BB := 13$

Знаходження ізогенії, яка відображає точки з E1 на E2 та представлена за допомогою раціонального відображення

```
> x:=5;y:=6;
```

$$x := 5$$

$$y := 6$$

```
> aa:=(x+(vq/(x-xq))+(uq/(x-xq)^2)) mod n;
```

$$aa := 8$$

```
> bb:=(y+(-uq*(2*y/(x-xq)^3))-(vq*((y-yq)/(x-xq)^2))+((gx*gy)/(x-xq)^2)) mod n;
```

$$bb := 5$$

$$E1(5,6) \rightarrow E2(8,5)$$

Точки переходять в точку на нескінченності для E2

```
> u:=(x^3-4*x^2-8*x-8)/(x^2-4*x+4) mod 19;
  v:=(x^3*y-6*x^2*y+5*x*y-6*y)/(x^3-6*x^2-7*x-8)mod 19;
```

$u := 8$

```
> x:=2;y:=12;
```

$v := 5$

$x := 2$

$y := 12$

```
> u:=(x^3-4*x^2-8*x-8)/(x^2-4*x+4) mod 19;
  v:=(x^3*y-6*x^2*y+5*x*y-6*y)/(x^3-6*x^2-7*x-8)mod 19;
Error, numeric exception: division by zero
Error, the modular inverse does not exist
> x:=2;y:=7;
> u:=(x^3-4*x^2-8*x-8)/(x^2-4*x+4) mod 19;
  v:=(x^3*y-6*x^2*y+5*x*y-6*y)/(x^3-6*x^2-7*x-8)mod 19;
```

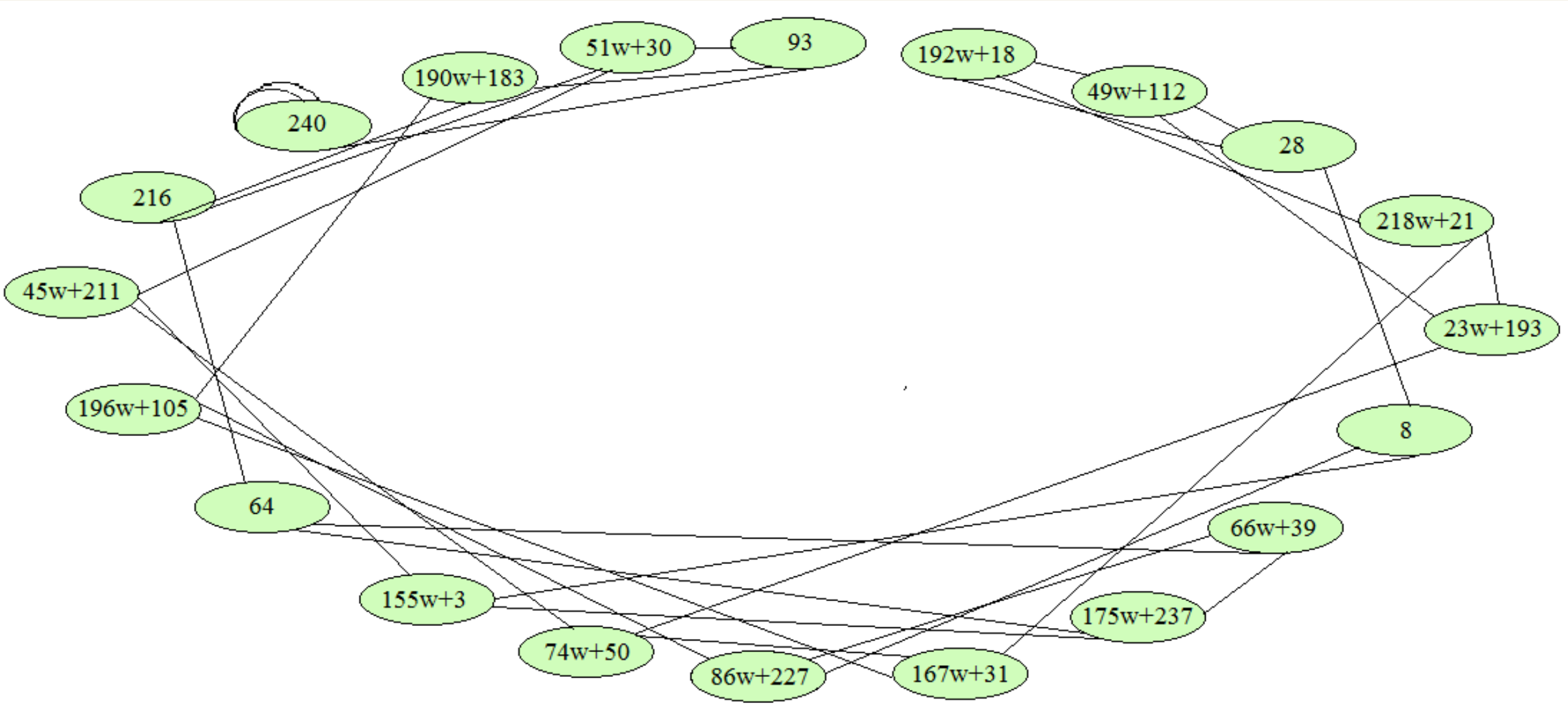
$x := 2$

```
Error, numeric exception: division by zero
```

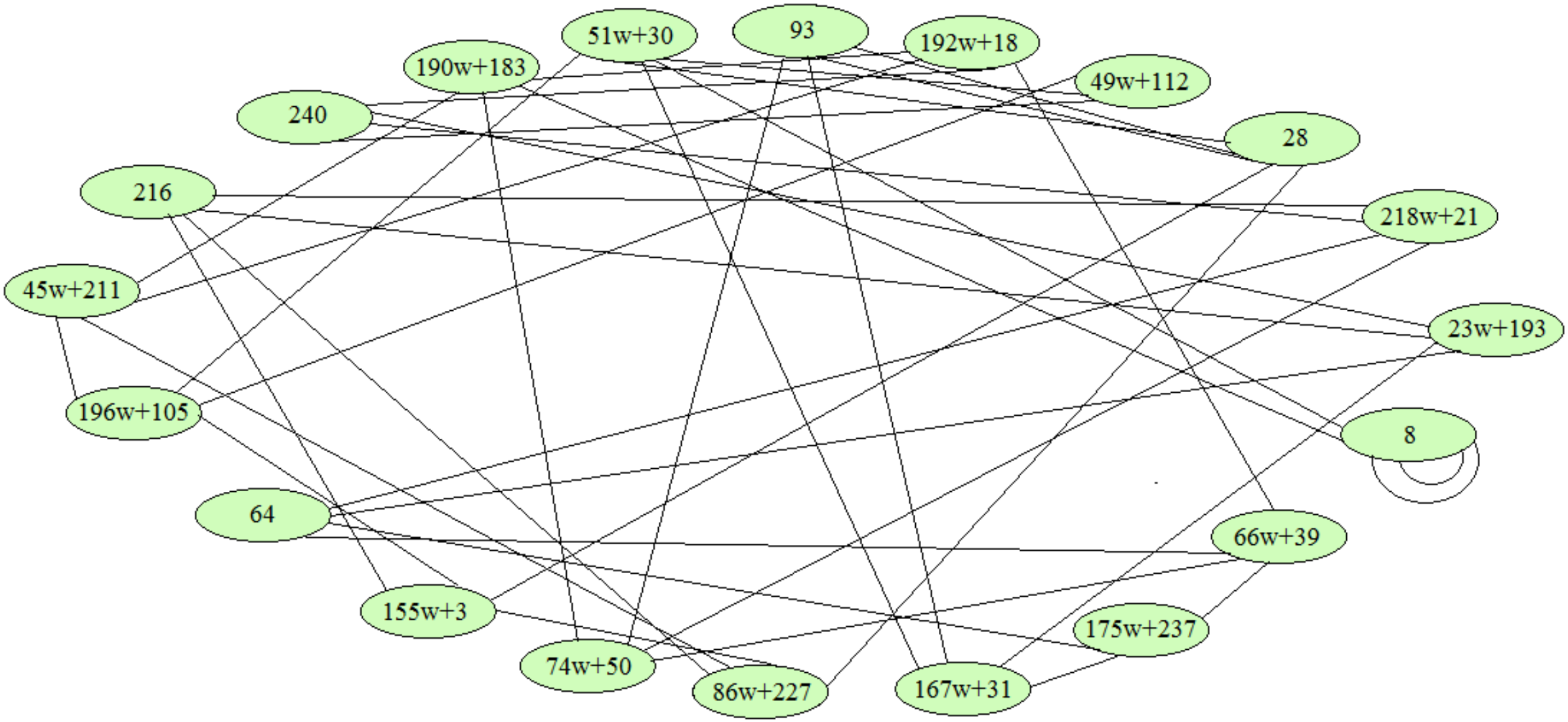
$y := 7$

```
Error, the modular inverse does not exist
```

ГРАФ ІЗОГЕНІЙ СУПЕРСИНГУЛЯРНИХ КРИВИХ

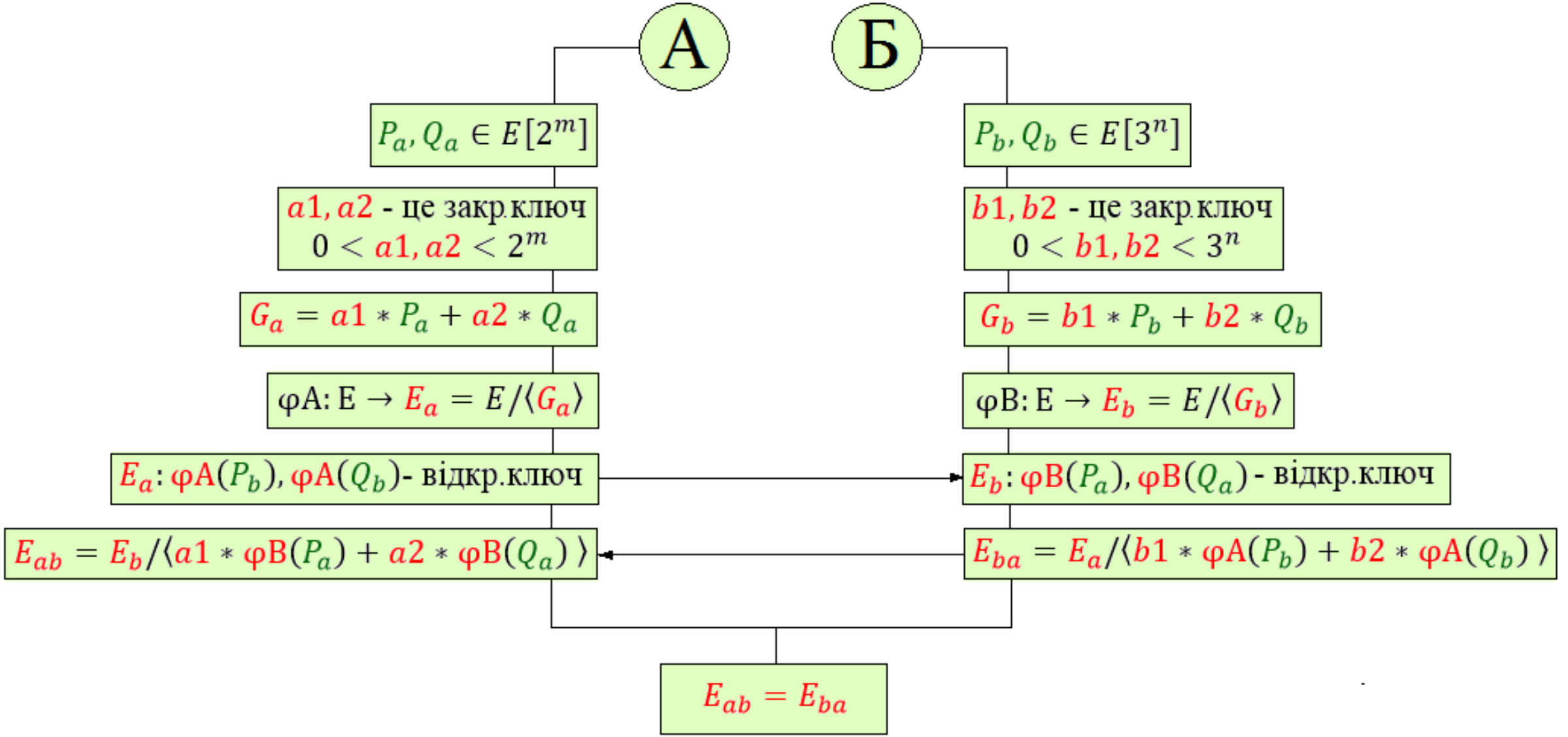


Для ізогенії ступеня 2 :
Кожна крива має 3 изогенії.



Для ізогенії ступеня 3 :
Кожна крива має 4 изогенії.

Схема алгоритму



ПЕРЕЛІК ПОСИЛАНЬ

1. Rostovtsev A., Stolbunov A. Public-Key Cryptosystem Based on Isogenies, Saint Petersburg, 2006 – 19 с.
2. Childs M. A., David Jao D., Soukharev V. Constructing elliptic curve isogenies in quantum subexponential time, 2010
3. David Jao, Luca De Feo, Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies, Canada, 2011 – 15 с.
4. Costello C., Longa P., Naehrig M.Efficient algorithms for supersingular isogeny Diffie-Hellman, USA, 2016 – 34с.
5. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография, СПб.: Профессионал, 2004. – 480 с.
6. О. Н. Василенко, Об алгоритмах построения изогений эллиптических кривых над конечными полями и их приложениях, Матем. вопр. криптогр., Москва, 2010. – том 1, выпуск 1, с. 7–22
7. Материал на сайте wipedia.org «Supersingular elliptic curve»
8. Материал на сайте wipedia.org «Supersingular isogeny key exchange»
9. Материал на сайте wipedia.org «Post-quantum cryptography»
10. Постквантовая реинкарнация алгоритма Диффи-Хеллмана: вероятное будущее (изогении)[Електронний ресурс], Олег Тараскін Режим доступу: https://habr.com/ru/company/aktiv-company/blog/332494
11. Luca De Feo, David Jao, Jérôme Plût Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies[Електронний ресурс], Cryptology ePrint Archive: Report 2011/506,- Режим доступу: https://eprint.iacr.org/2011/506
12. Craig Costello, Patrick Longa, Michael Naehrig Efficient algorithms for supersingular isogeny Diffie-Hellman[Електронний ресурс], Cryptology ePrint Archive: Report 2016/413,- Режим доступу: https://eprint.iacr.org/2016/413
13. Гайтота Є.В. Ізогенії на еліптичних кривих
14. Craig Costello, David Jao, Patrick Longa, Michael Naehrig, Joost Renes, David Urbanik Efficient compression of SIDH public keys[Електронний ресурс], Cryptology ePrint Archive: Report 2016/963- Режим доступу: https://eprint.iacr.org/2016/963
15. Craig Costello, Huseyin Hisil A simple and compact algorithm for SIDH with arbitrary degree isogenies[Електронний ресурс], Cryptology ePrint Archive: Report 2017/504 - Режим доступу: https://eprint.iacr.org/2017/504
16. SIDH Library[Електронний ресурс], Established: April 16, 2016 - Режим доступу: https://www.microsoft.com/en-us/research/project/sidh-library/
17. Luca De Feo Mathematics of Isogeny Based Cryptography[Електронний ресурс] - Режим доступу: https://arxiv.org/pdf/1711.04062.pdf
18. А. Пономар Особливості та проблематика створення криптографічних систем, заснованих на використанні ізогеній еліптичних кривих, ISSN 0485-8972,Радиотехника. 2016.Вып. 18696УДК 004.056.55.

Дякуємо за увагу!