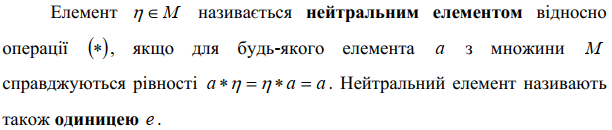
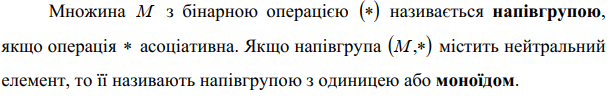
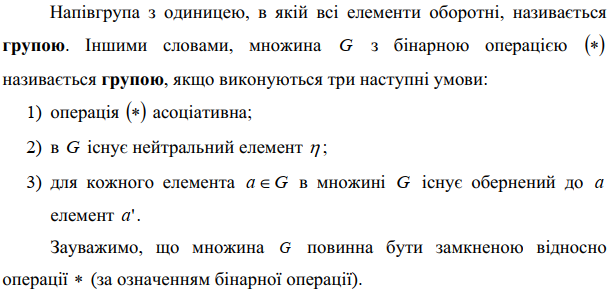
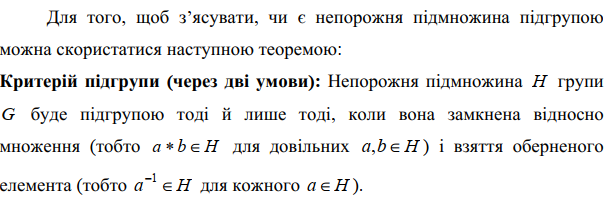
1. **Означення напівгрупи та групи. Нейтральний елемент групи. (ст. 6-7)**

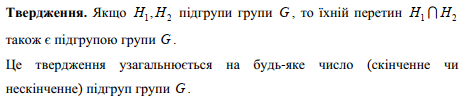
****

****

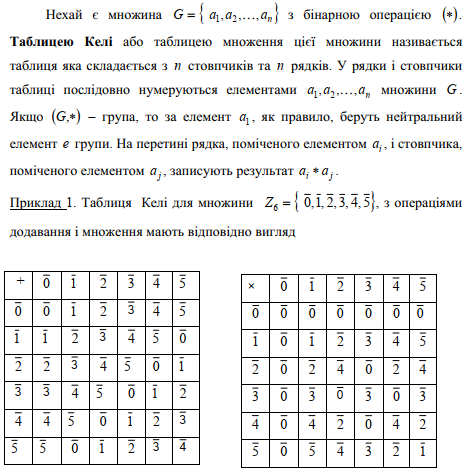
****

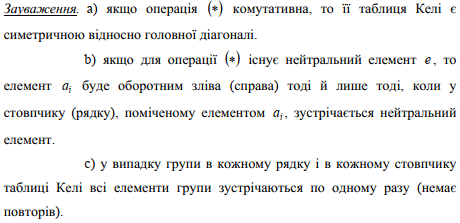
1. ***Критерій підгрупи.(ст.11)***

****

****

1. ***Таблиця Келі групи. Побудова таблиці Келі двох груп з чотирьох елементів.***

****

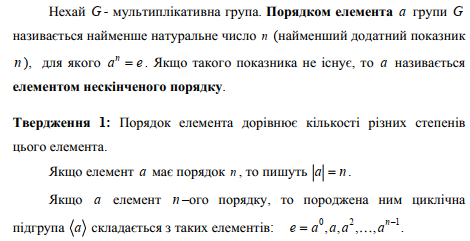
****

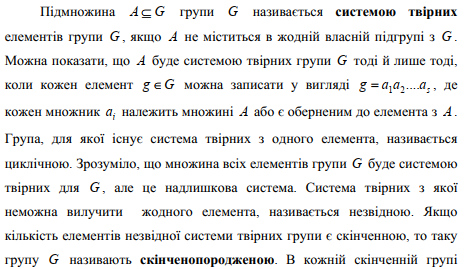
1. ***Порядок елемента групи. Циклічні групи. Система твірних елементів групи.(ст. 17,24-25)***

***Порядок групи це найменше n до якого вкинується а в степені n = e.***

***Циклічна група це група породжена якимось генератором групи.***

***Система твірних елементів групи це підмножена деякої групи. Кожний елемент цієї групи можна подати у вигляду а1 на а2 і так далі на аn. (З неї шяхом застосування операції групового елемента і взяття оберненого ми можемо створити цю множину).***

****

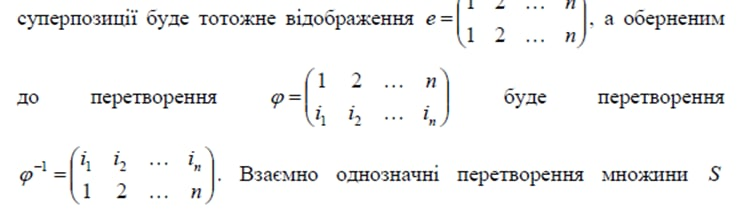
****

1. ***Група перестановок. Побудова оберненої перестановки. Парність перестановки.***

***Множина Sn всіх взаємно однозначних перетворень множини S = {1,2,…,n} утворює групу відносно композиції відображень. Такі взаємно однозначні перетворення називаються перестановками.***

***Перестановка називається парною, якщо загальна кількість інверсій її чисел є парною, і називається непарною в іншому випадку.***

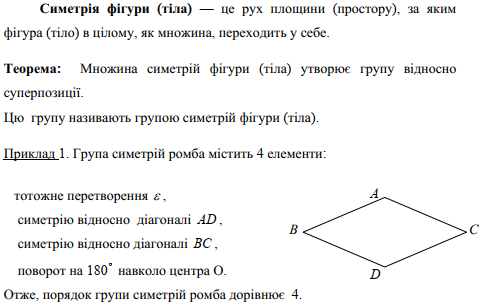


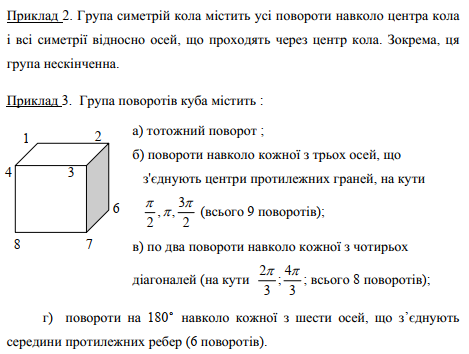


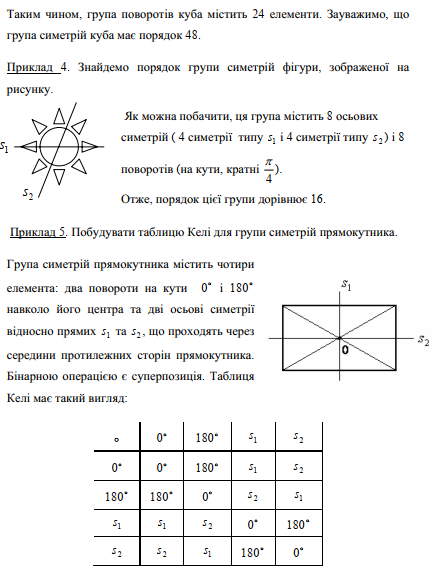


1. ***Групи симетрій. Приклади груп симетрій.(ст. 22)***

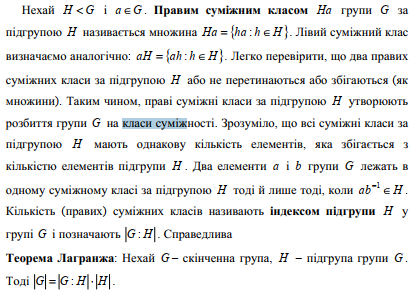
***Це відображення площини, коли фігура повертається сама в себе.***

****

****

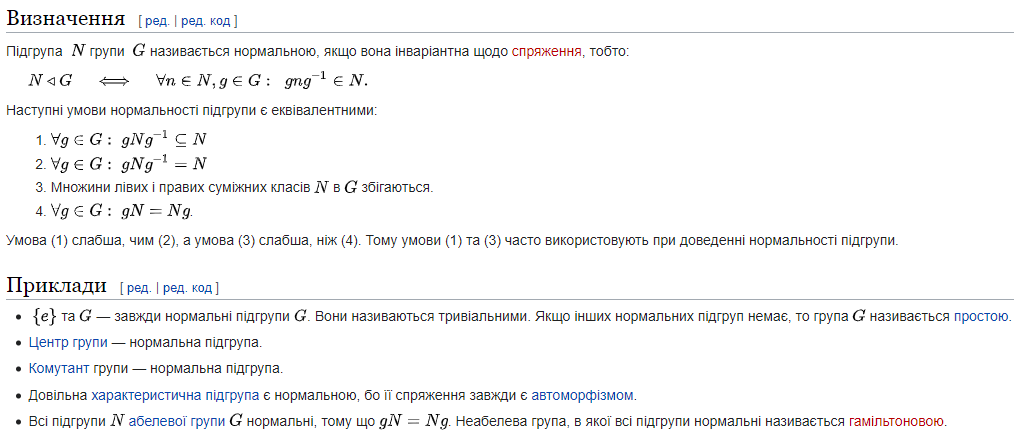
****

1. ***Класи суміжності. Нормальнi пiдгрупи. Фактор-групи (ст. 12 + вікіпедія)***

****

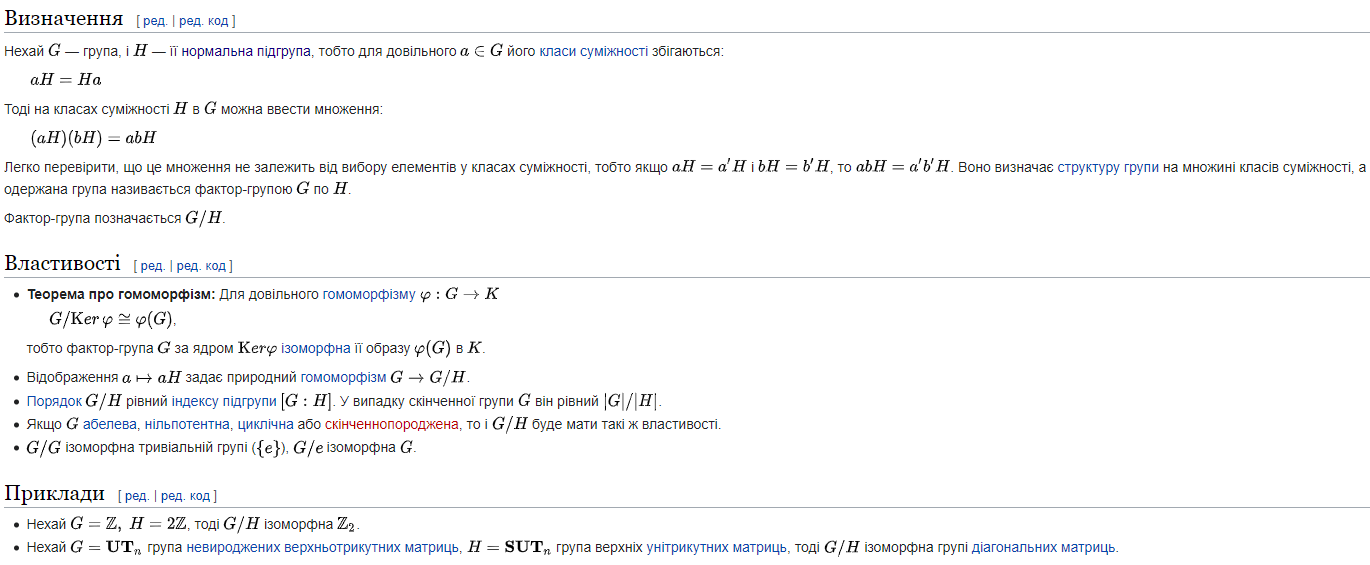
[***https://uk.wikipedia.org/wiki/Нормальна\_підгрупа***](https://uk.wikipedia.org/wiki/%D0%9D%D0%BE%D1%80%D0%BC%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%BF%D1%96%D0%B4%D0%B3%D1%80%D1%83%D0%BF%D0%B0)

****

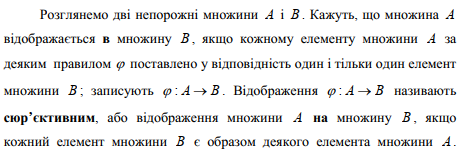
****

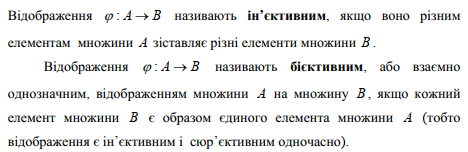
[***https://uk.wikipedia.org/wiki/Фактор-група***](https://uk.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80-%D0%B3%D1%80%D1%83%D0%BF%D0%B0)

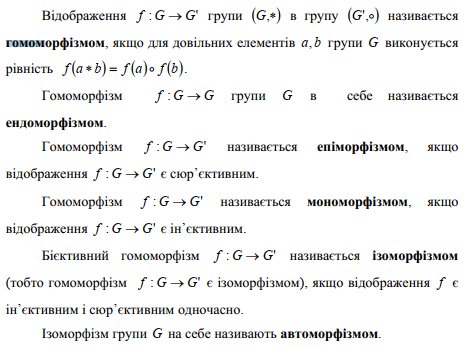
****

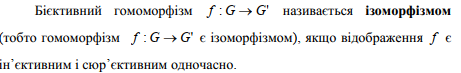
****

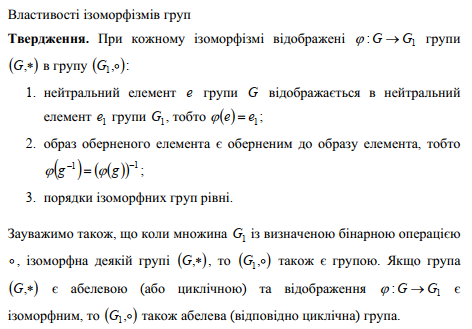
1. ***Гомоморфізм, ізоморфізм.(ст. 28-31)***

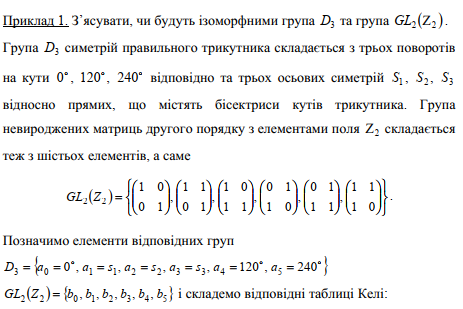
****

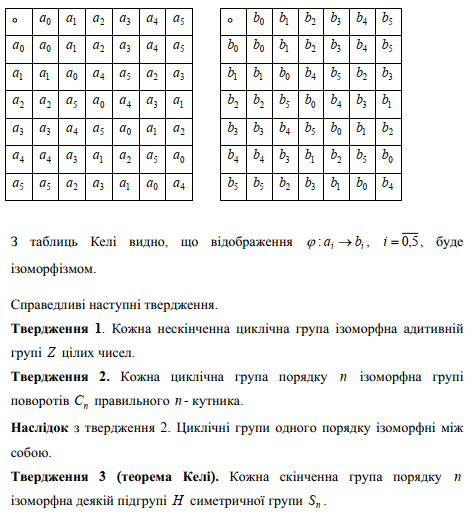
****

****

****

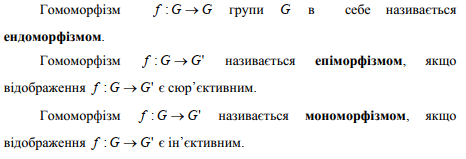
****

****

****

1. ***Eпіморфізм, мономорфізм, автоморфізм.(ст. 29)***

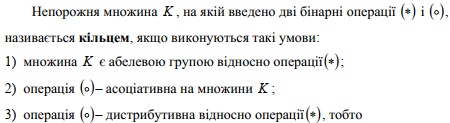
***Все це йде з гомоморфізму. Гомоморфізм це відображення з групи в групу в яких різні групові операції. Епіморфізм це гомоморфізм який є сюр’єктивним (може приймате всі можливі значення). Мономорфізм це гомоморфізм який є ін’єктивним (***то есть если два [образа](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%80%D0%B0%D0%B7_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)) при отображении совпадают, то и [прообразы](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BE%D0%B1%D1%80%D0%B0%D0%B7) совпадают***). Автоморфіз це бієктивний гомоморфізм(ізоморфізм) самої на себе.***

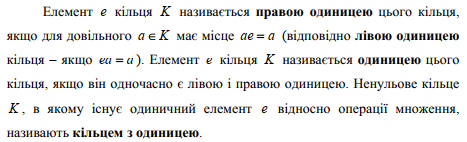
****

****

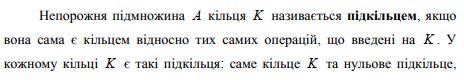
1. ***Означення кільця. Кільце з одиницею. (ст. 34)***

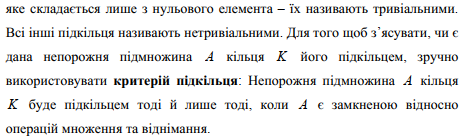
***Чи буде множина усіх скінченних многочленів кільцем? Так, тому-що не існує оберненого елемента.***

****

****

1. ***Критерій підкільця. (ст. 35-36)***

****

****

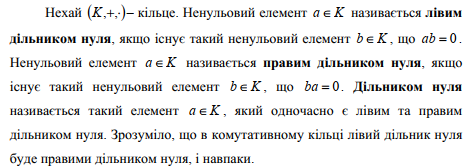
1. ***Лівий та правий дільники нуля. Лівий та правий дільник одиниці. (ст. 40)***

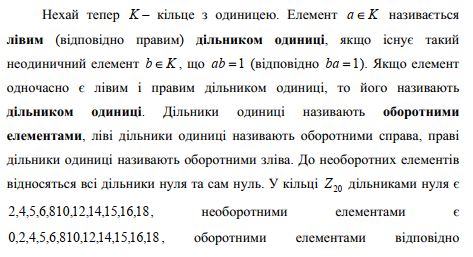
***Якщо А на Б то Б лівий дільник нуля.***

***Дільники нуля в полі бути не можуть.***

***Дільники нуля в кільці бути можуть.***

***Кільце по модулю 10. 2,4,5,6,8.***

****

****

****

1. ***Область цілісності. Поле. Характеристика поля. Генератори мультиплікативної групи поля. (ст. 40-41)***

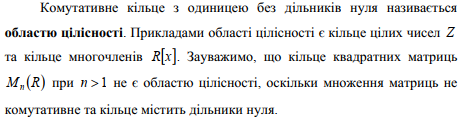
***Область цілісності це комутативне кільце з одиницею без дільників нуля.***

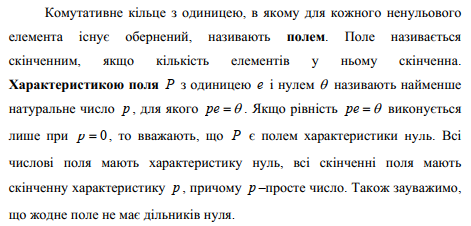
***Поле це комутативне кільце з одиницею, в якому для кожного ненульового елемента існує обернений.***

***В нас є одиниця і нуль, характеристикою поля називається таке найменше число, для якого число помножене на одиницю = нашому нулю. Якщо це виконується лише при нулю, то Р є полем характеристики нуль. Р – просте число. Поле не має дільників нуля.***

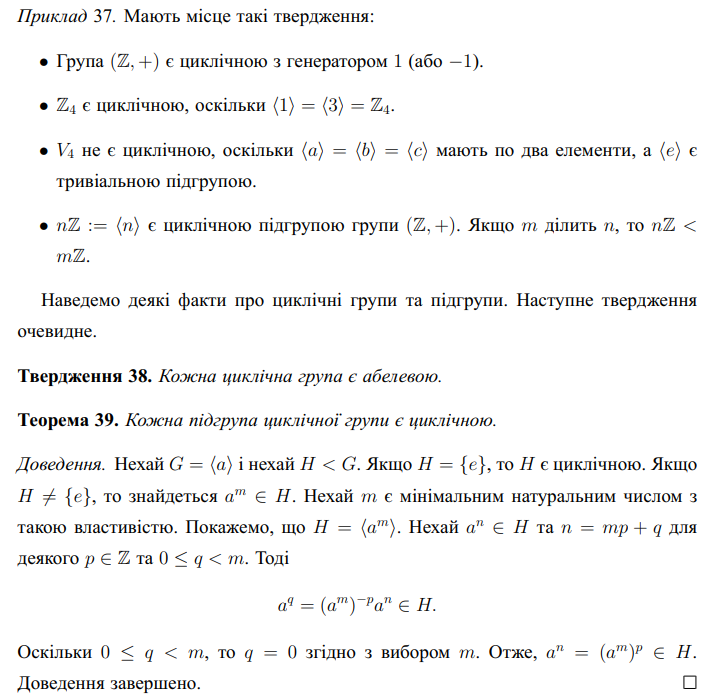
***Z13. Характеристика = 13(скільки ми додали одиницю разів). 4 Генератори за ф.Ейлера***

***Елемент називається генератором якщо він породжує групу, елементами групи є степені.***

****

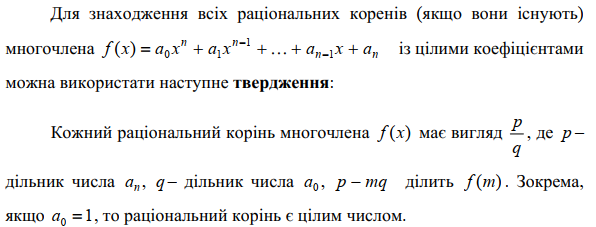
****



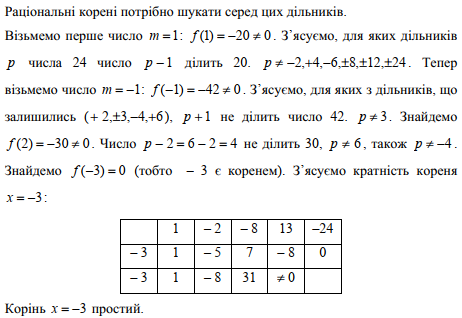


1. ***Описати метод знаходження раціональних коренів многочлена.(57-58)***

***У нас є якийсь многочлен А0 це перший коеф. An останній. Р це дільник числа An, q – дільник числа а0. Потім ми вибираємо число m так що p-mq ділить f(m). Якщо не ділить, то ми ці дільники які були відкидаємо і перевіряємо нове m.***

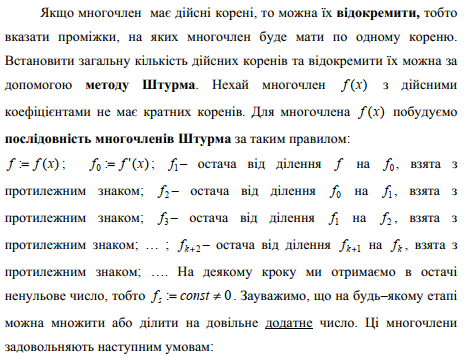
****

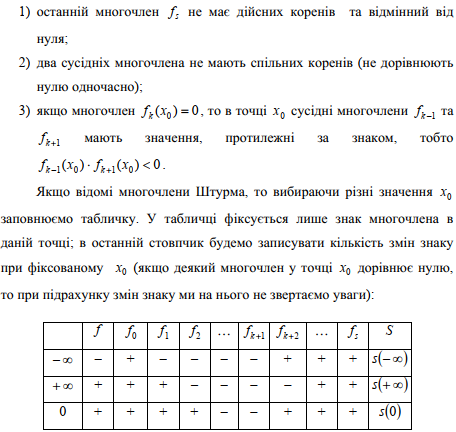
****

****

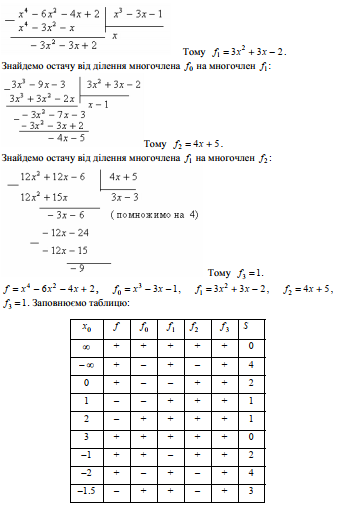
1. ***Описати метод Штурма. Для чого він використовується?(ст. 58-61)***

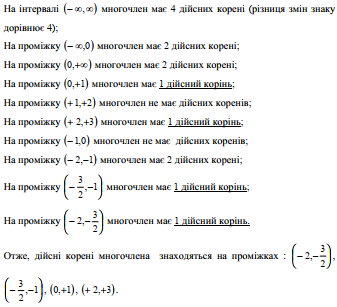
***Він використовується для пошуку коренів відрізка. У нас є многочлен ф(х). Спочатку ми знаходимо його похідну, далі присвоїмо ф0(х) як остачу від ділення ф(х) на ф’(х). Далі аналогічно робимо для ф1(х) (ф1(х) це остача від ділення ф0(х) на -ф’(х)) і т.д. поки не дойдемо до константи. Далі ми беремо початок відрізка і кінець відрізка і наприклад для якогось х0 ми рахуємо значення цих всіх многочленів в т. х0 і рахуєм кількість змін знаку в цій послідовності. І різниця цих знаків між різними х0 і буде кількість дійсних коренів у цьому відрізку.***

****

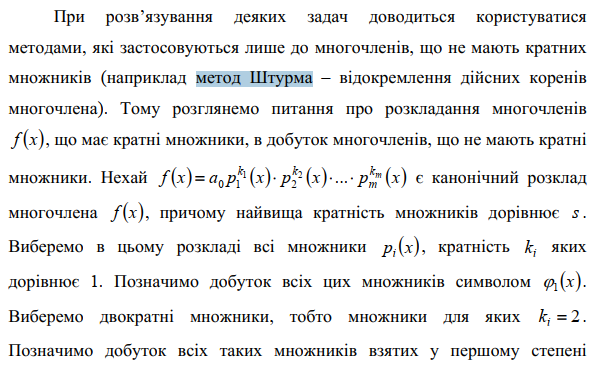
****

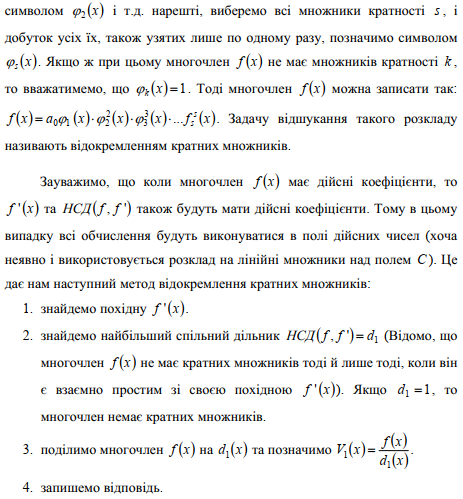
****

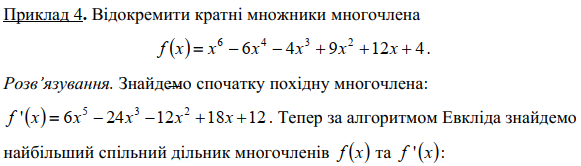
****

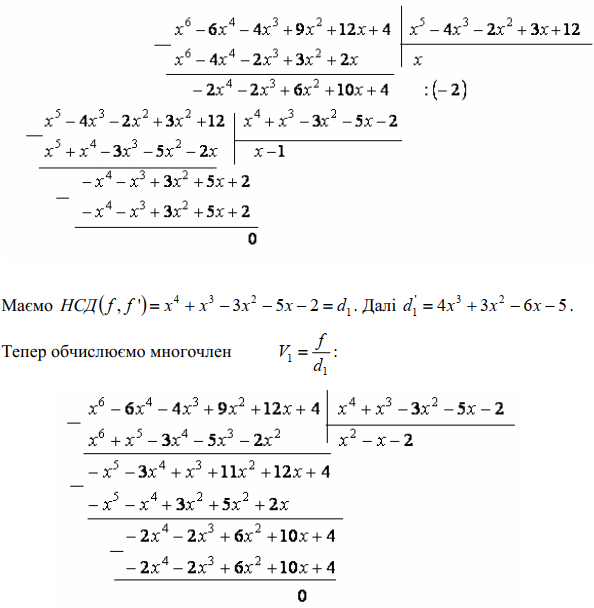
****

1. ***Описати спосіб виокремлення кратних коренів многочлена.(ст. 61-63)***

****

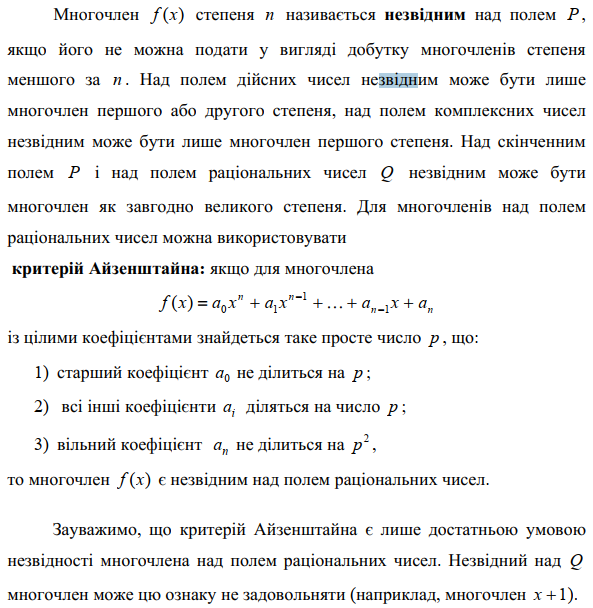
****

****

****

****

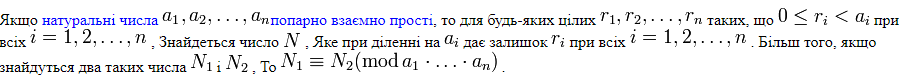
1. ***Звідні та незвідні многочлени. Вигляд незвідних многочленів над полями дійcних та комплексних чисел.***

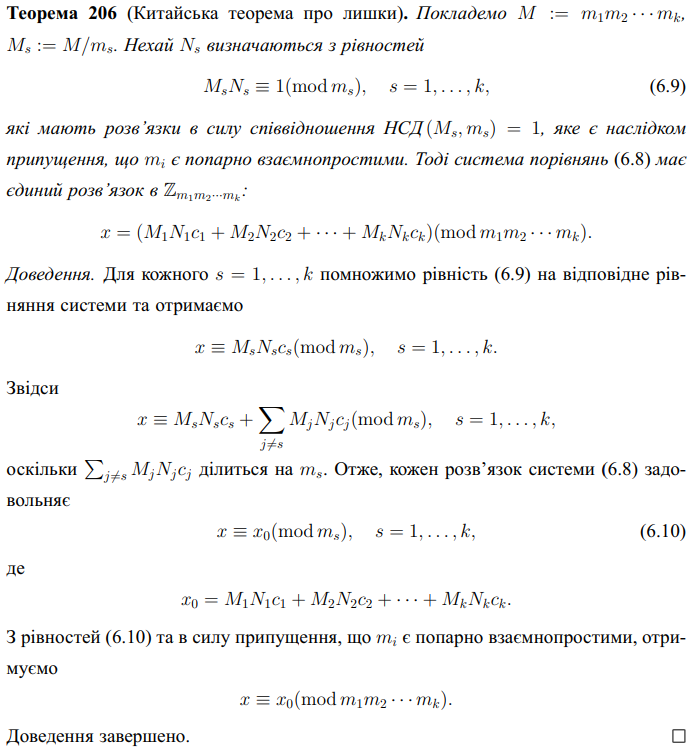
****

****

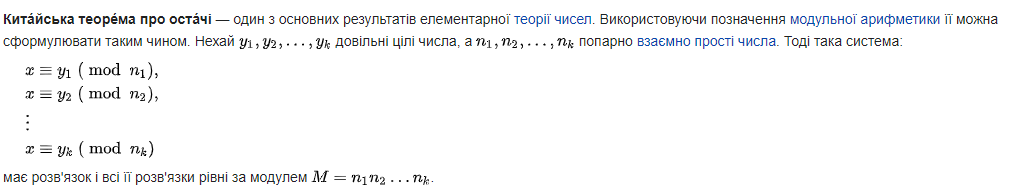
1. ***Китайська теорема про лишки.***

[***https://znaimo.com.ua/Китайська\_теорема\_про\_залишки***](https://znaimo.com.ua/%D0%9A%D0%B8%D1%82%D0%B0%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D1%82%D0%B5%D0%BE%D1%80%D0%B5%D0%BC%D0%B0_%D0%BF%D1%80%D0%BE_%D0%B7%D0%B0%D0%BB%D0%B8%D1%88%D0%BA%D0%B8)

****



[***https://uk.wikipedia.org/wiki/Китайська\_теорема\_про\_остачі***](https://uk.wikipedia.org/wiki/%D0%9A%D0%B8%D1%82%D0%B0%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D1%82%D0%B5%D0%BE%D1%80%D0%B5%D0%BC%D0%B0_%D0%BF%D1%80%D0%BE_%D0%BE%D1%81%D1%82%D0%B0%D1%87%D1%96)

****

1. ***Функція Мьобіуса. Згортка Діріхле. Формула Мьобіуса для обернення.***

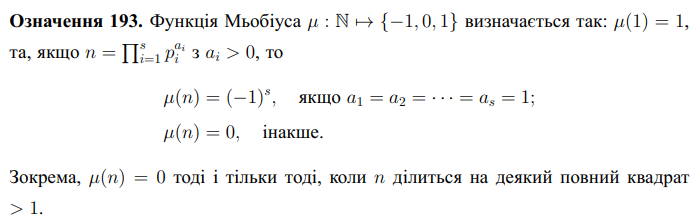
***Формула Мьобіуса дає результат чи ділиться число на якийсь квадрат. Якщо число розкладається як р1 на р2 на р3 та р може повторятися то результат ми отримаємо як***

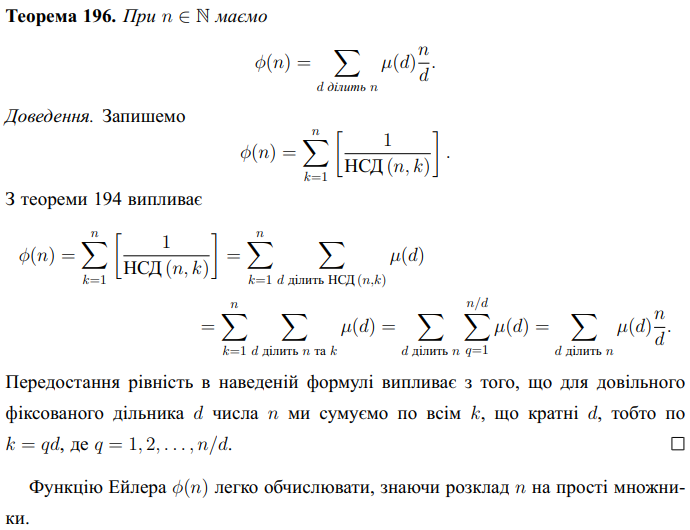
***-1 в степені S де S – кількість коренів і якщо у нас хоча б один повний квадрат знайдеться то ми повертаєм нуль.***

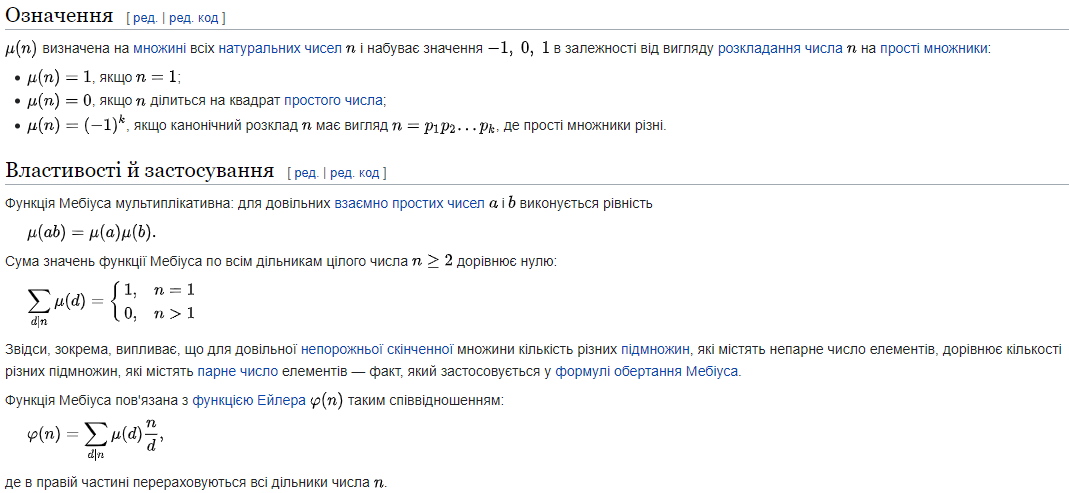
***Згортка Діріхле допомагає порахувати суму по А\*Б=Н, де А та Б – довільні Ф(А)\*Ж(Б)***

***Це окремий випадок функції Діріхле.***

[***https://uk.wikipedia.org/wiki/Функція\_Мебіуса***](https://uk.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%8F_%D0%9C%D0%B5%D0%B1%D1%96%D1%83%D1%81%D0%B0)

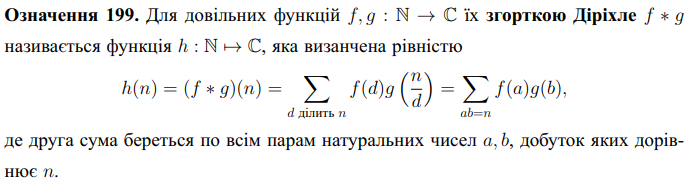


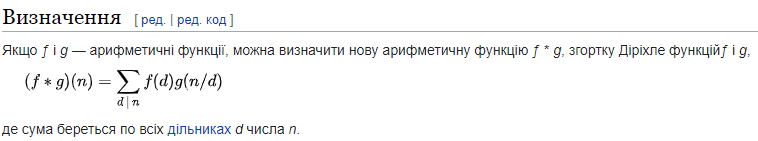


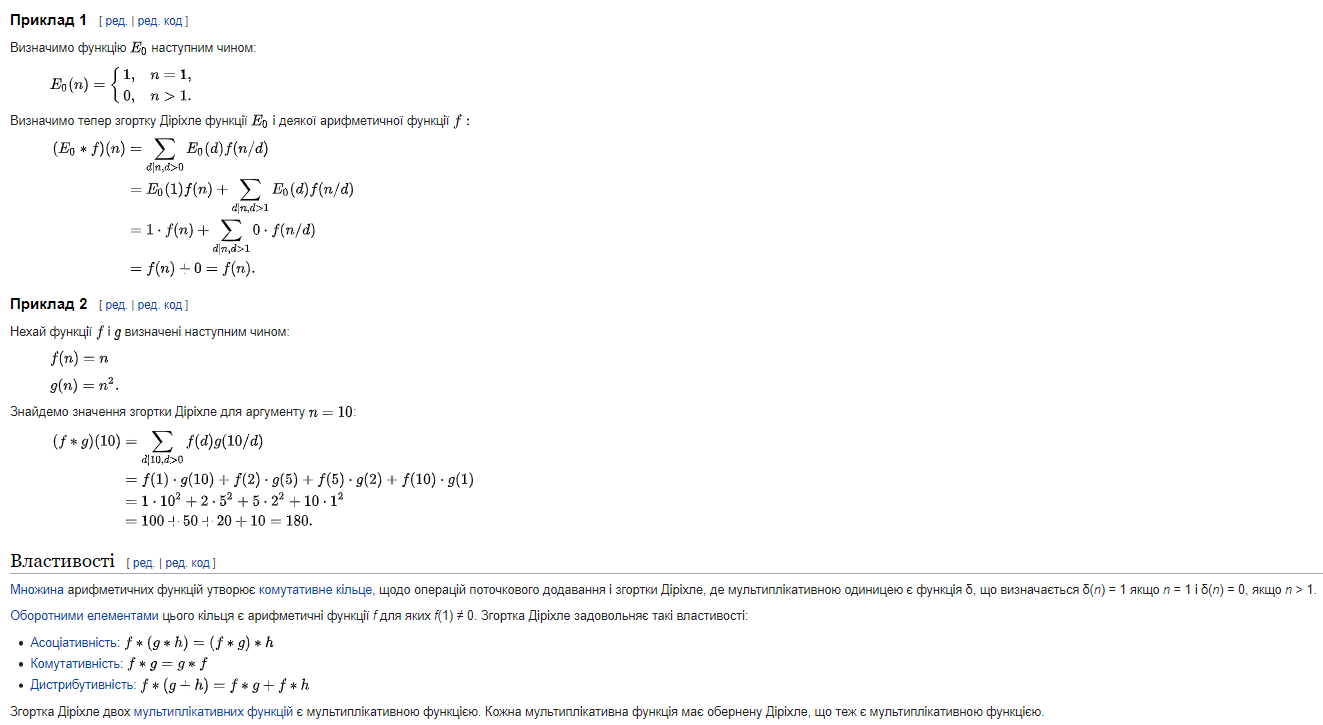
****

[***https://uk.wikipedia.org/wiki/Згортка\_Діріхле***](https://uk.wikipedia.org/wiki/%D0%97%D0%B3%D0%BE%D1%80%D1%82%D0%BA%D0%B0_%D0%94%D1%96%D1%80%D1%96%D1%85%D0%BB%D0%B5)

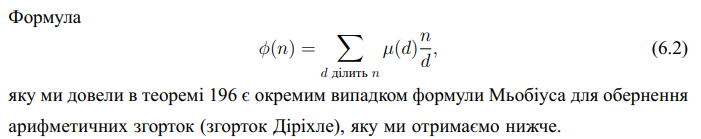
****

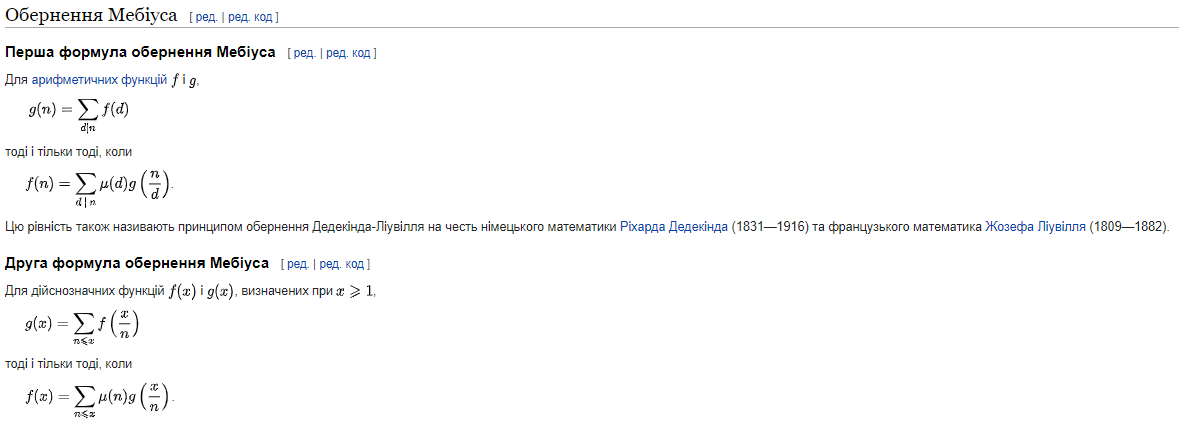


****

****

[***https://uk.wikipedia.org/wiki/Функція\_Мебіуса***](https://uk.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%8F_%D0%9C%D0%B5%D0%B1%D1%96%D1%83%D1%81%D0%B0)



****

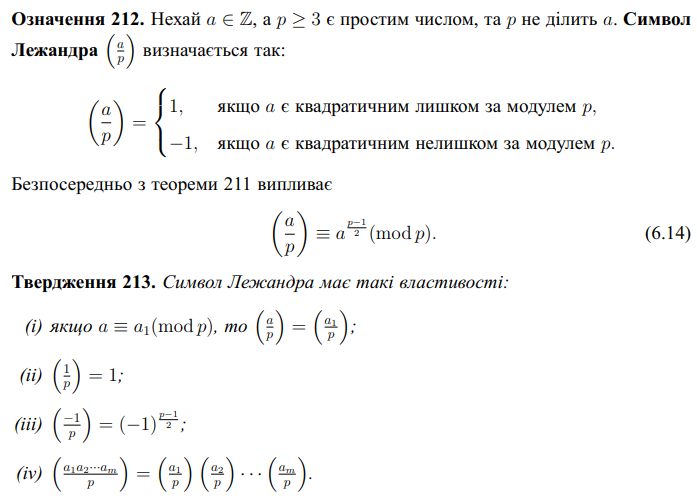
1. ***Символи Лежандра і Якобі та їх властивості.***

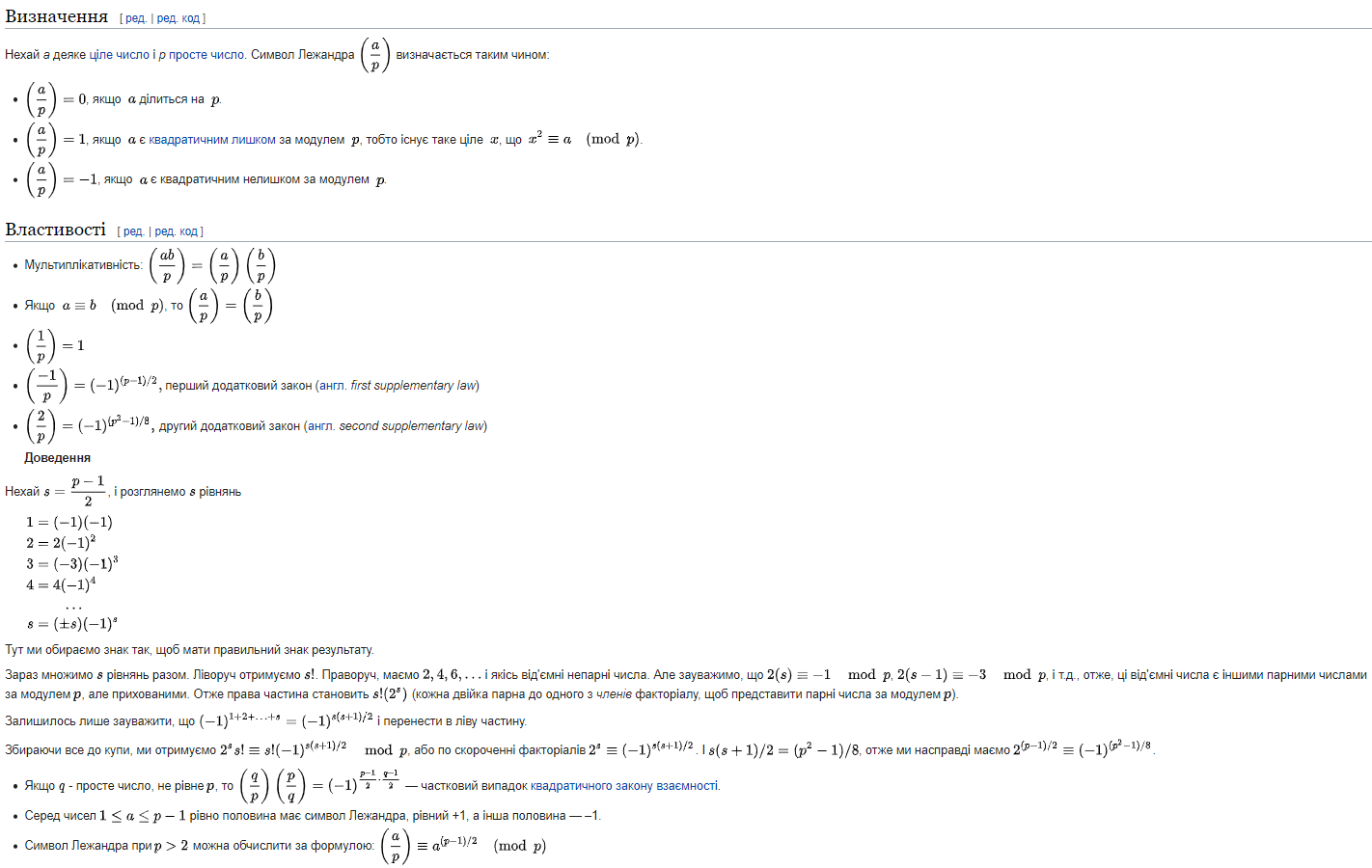
***Символ Лежандра це часний випадок символа Якобі. Він використовується для багатьох алгоритмів. Символ Лежандра це функція яка повертає залежності від числа 0, 1 або -1 якщо число А ділиться на модуль числа. Тобто повертає 0 коли А ділиться на Б. Повертає 1 коли А є квадратним лишком по модулю, і -1 коли не є квадратним лишком.***

***Символ Якобі. Мультиплікативність, періодична по досліджуємій змінній. Основні властивості від одиниці завжди одиниця, від -одиниці в степені число ((модуля-1)/2). Так як Б це просте число, ми зробимо його найменше значення і ділимо на 2.***

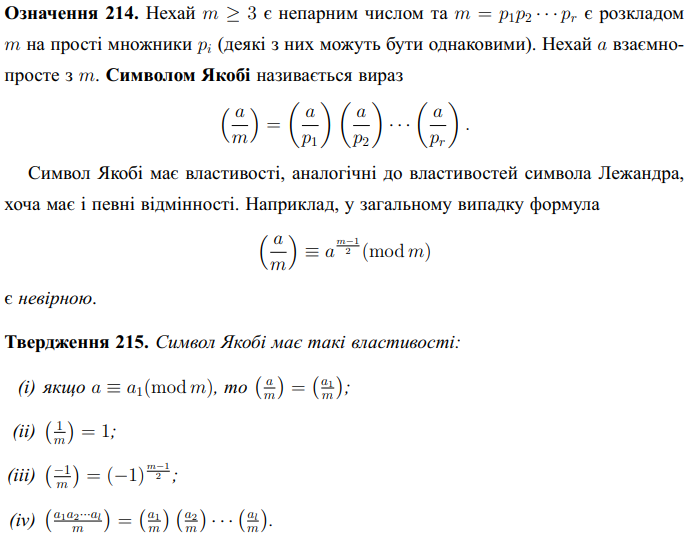
***Для того щоб обрахувати символ Якобі через символ Лежандра ми розкладуємо знаменник на прості множники і якщо є більше ніж один множник степеня 2 або вище то він повертає 0***

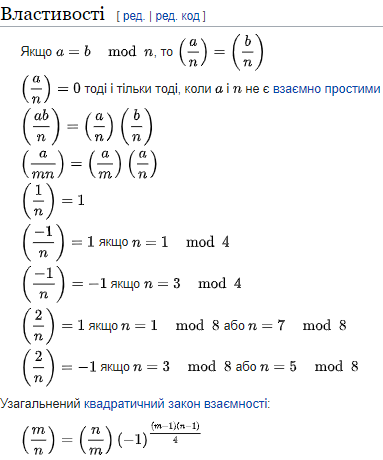
****



****

****

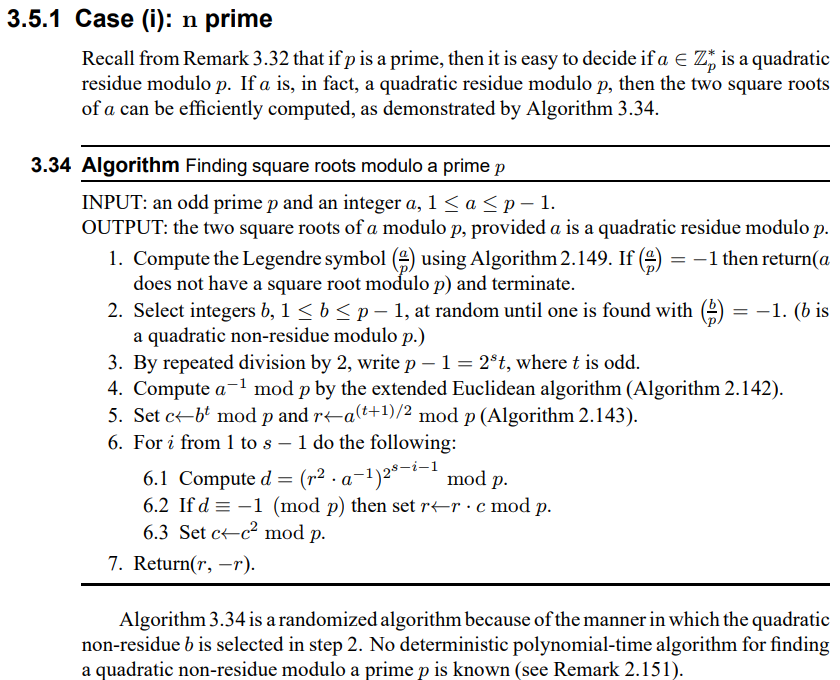


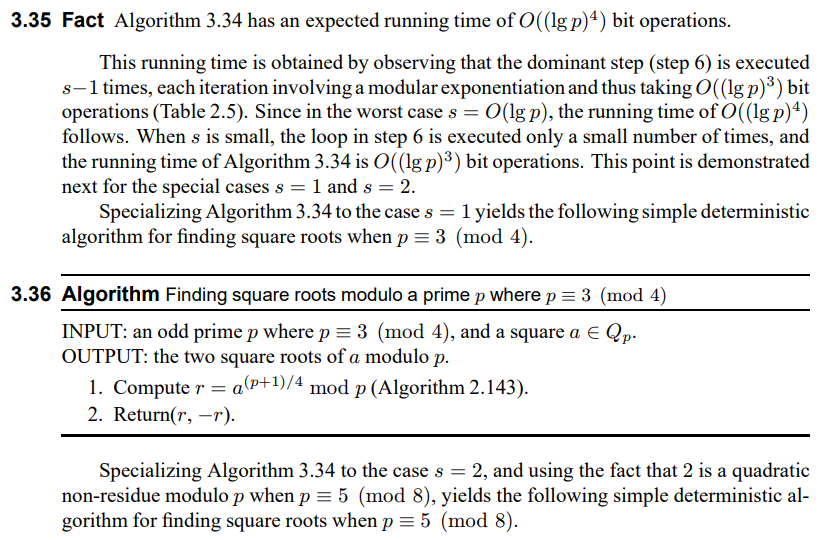
****

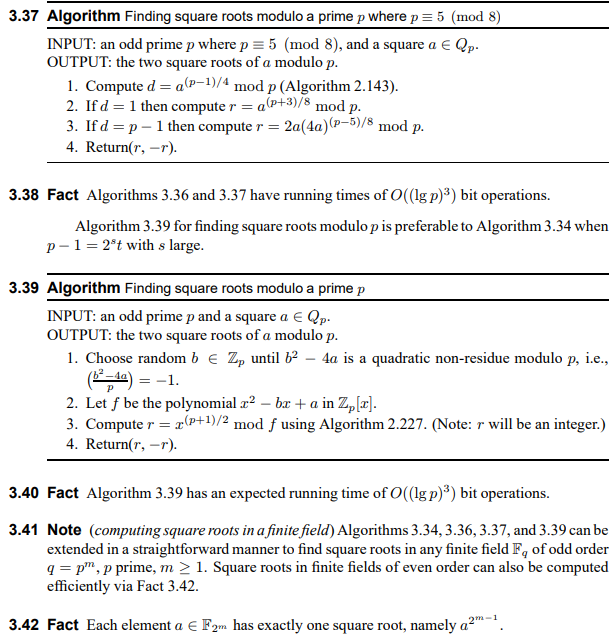
1. ***Описати алгоритм знаходження квадратного кореня числа у скінченному полі.***

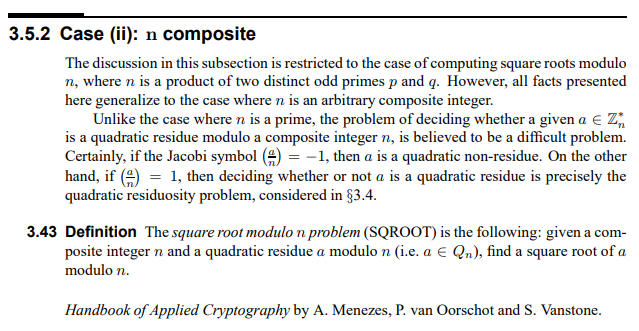
***Нехай у нас є число x^2 mod p. Ми шукаємо х. Спочатку b повинен бути квадратним лишком за модулем р. Ми вибираєсо випадкове число з цього поля так що b^2 – a = 0, то ми можемо повертати р як з + так із -. Тому-що ми знайшли квадратний корінь. Далі ми дивимось, якщо b^2 є квадратним лишком, повертаємось назад і змінюємо А на нове число b^2 – a. І робимо так поки не знайдемо квадратний корінь. Складність (p-1)/2. Ймовірність того що ми виберемо елемент і він буде квадратним лишком – 50%.***

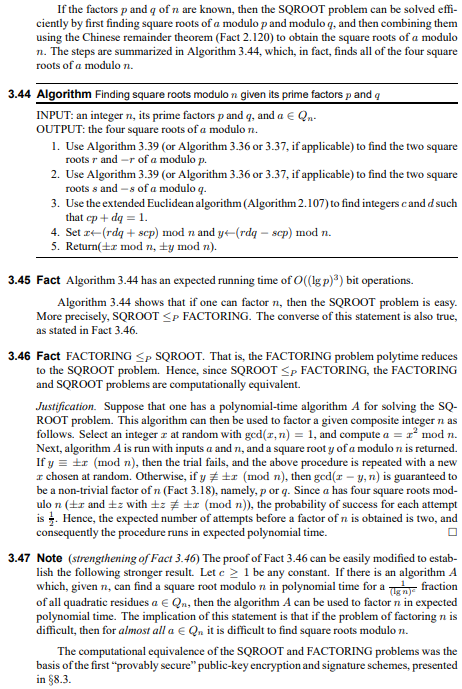
[***https://cacr.uwaterloo.ca/hac/about/chap3.pdf***](https://cacr.uwaterloo.ca/hac/about/chap3.pdf) ***(ст. 99-102 (14-17))***



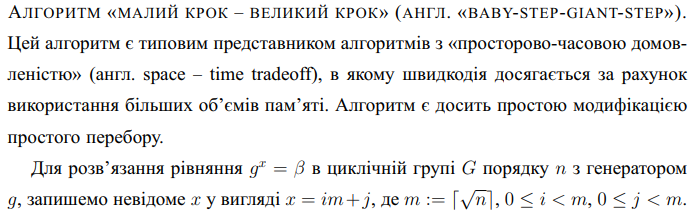


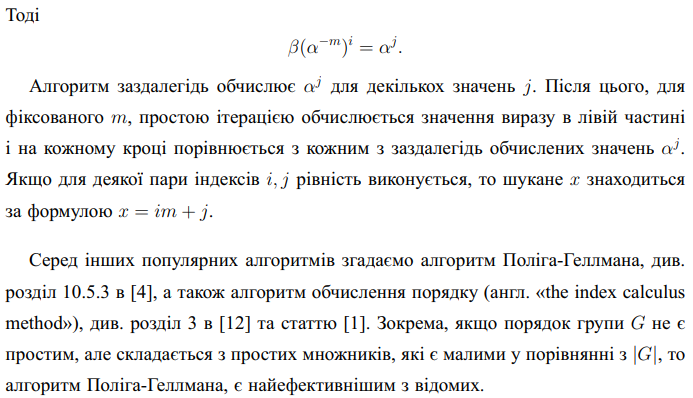




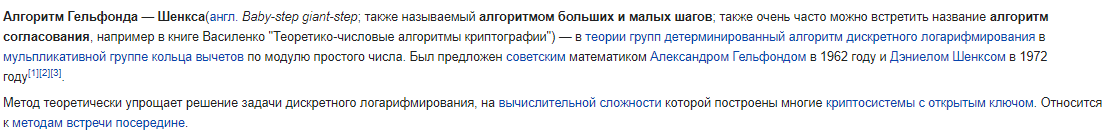


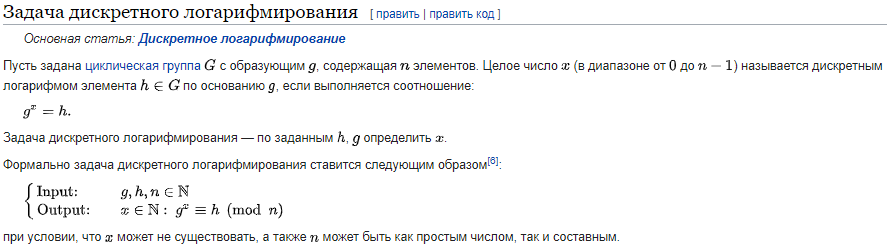
1. ***Описати алгоритм знаходження дискретного логарифму числа у скінченному полі за допомогою алгоритму baby-step giant-step.***

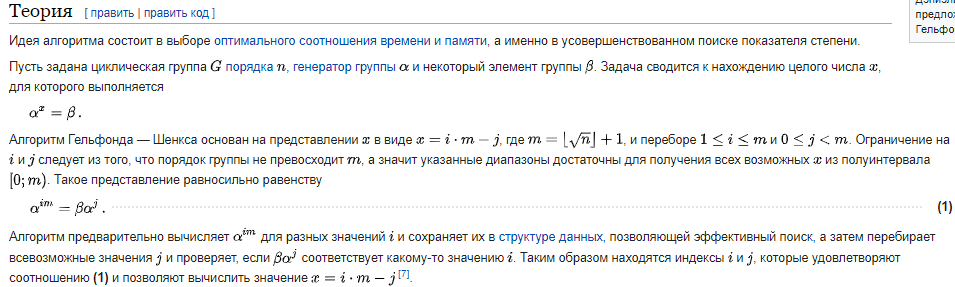




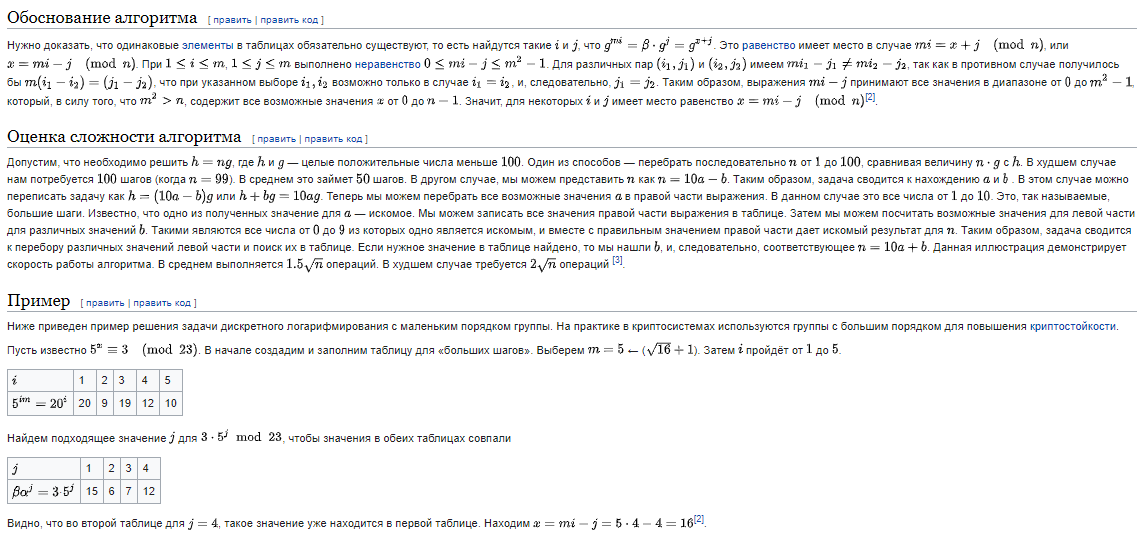
[***https://ru.wikipedia.org/wiki/Алгоритм\_Гельфонда\_—\_Шенкса***](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%93%D0%B5%D0%BB%D1%8C%D1%84%D0%BE%D0%BD%D0%B4%D0%B0_%E2%80%94_%D0%A8%D0%B5%D0%BD%D0%BA%D1%81%D0%B0)



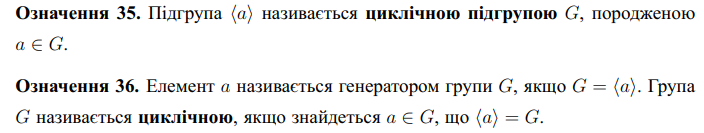


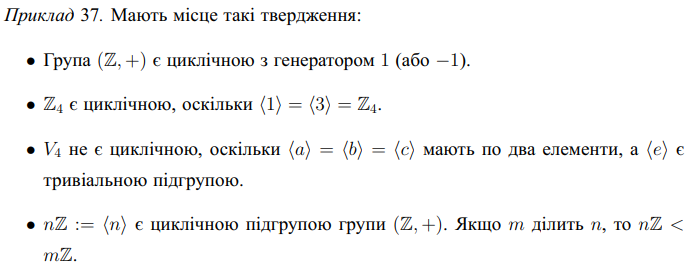


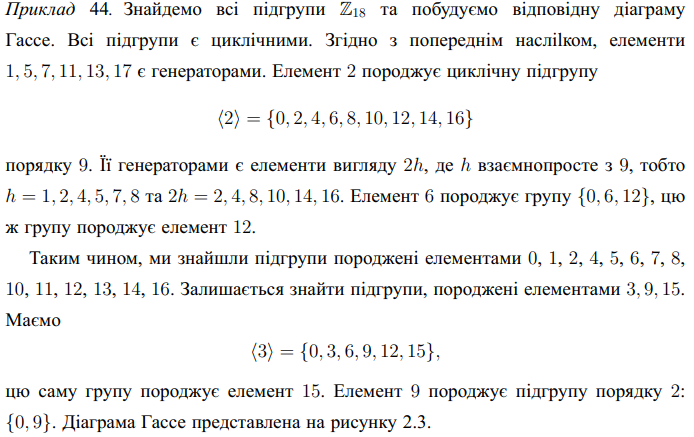




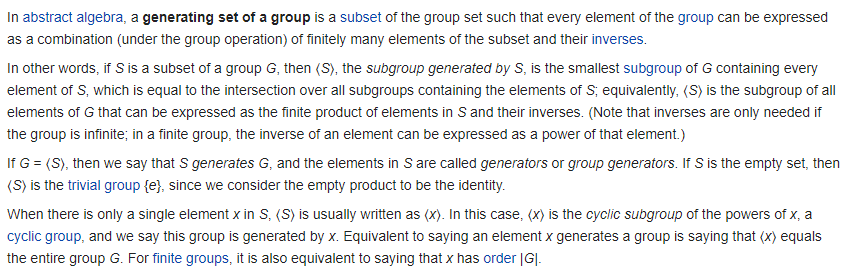
1. ***Генератор мультиплікативної групи поля, їх кількість. Означення та застосування функції Ейлера та Каймаркла. Алгоритм знаходження генератора.***

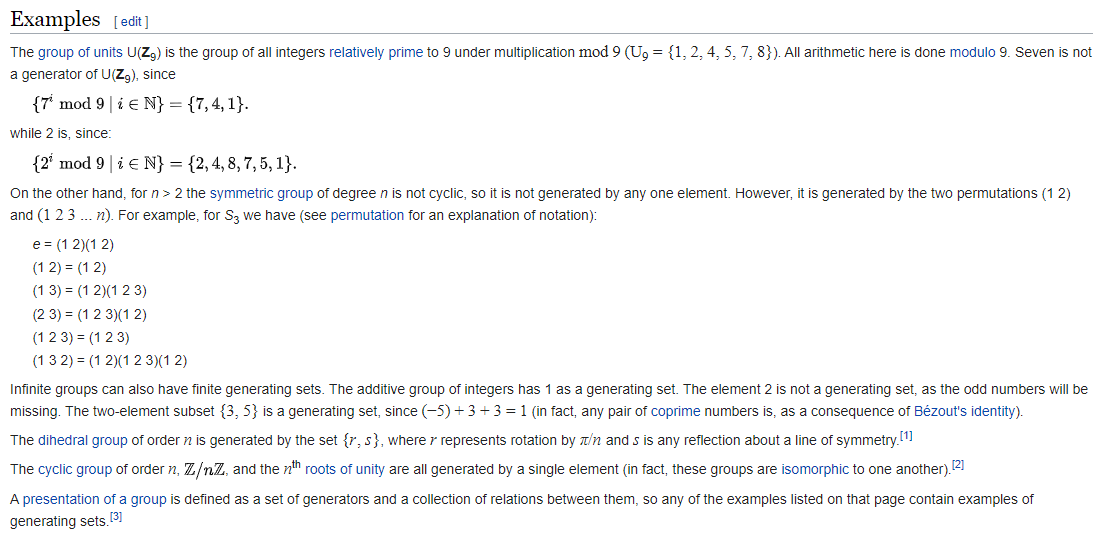


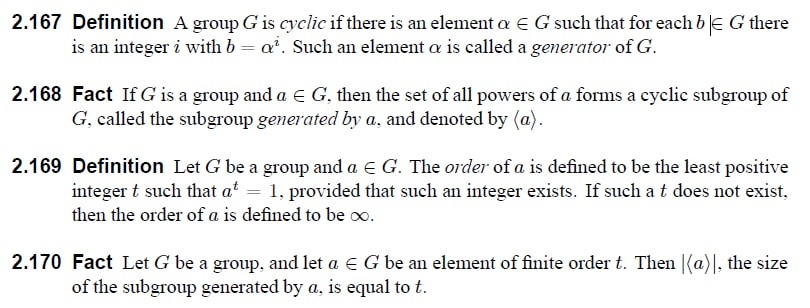
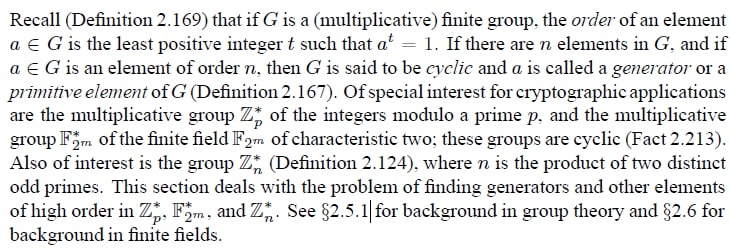


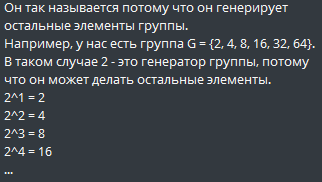


[***https://en.wikipedia.org/wiki/Generating\_set\_of\_a\_group***](https://en.wikipedia.org/wiki/Generating_set_of_a_group)



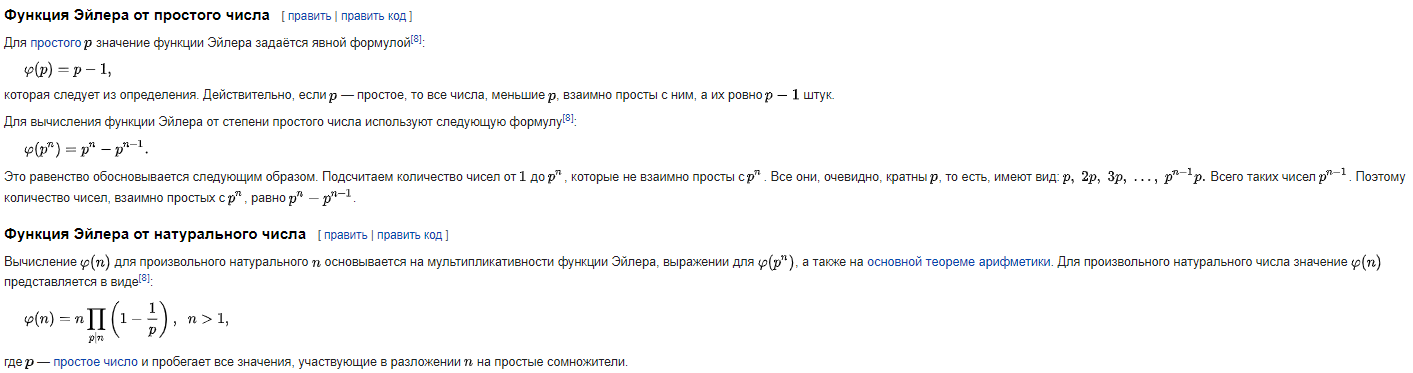




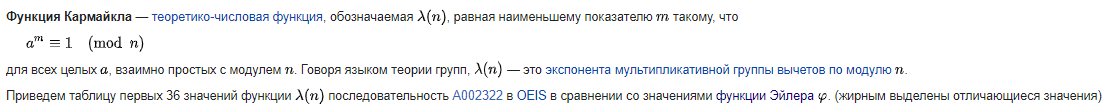
 

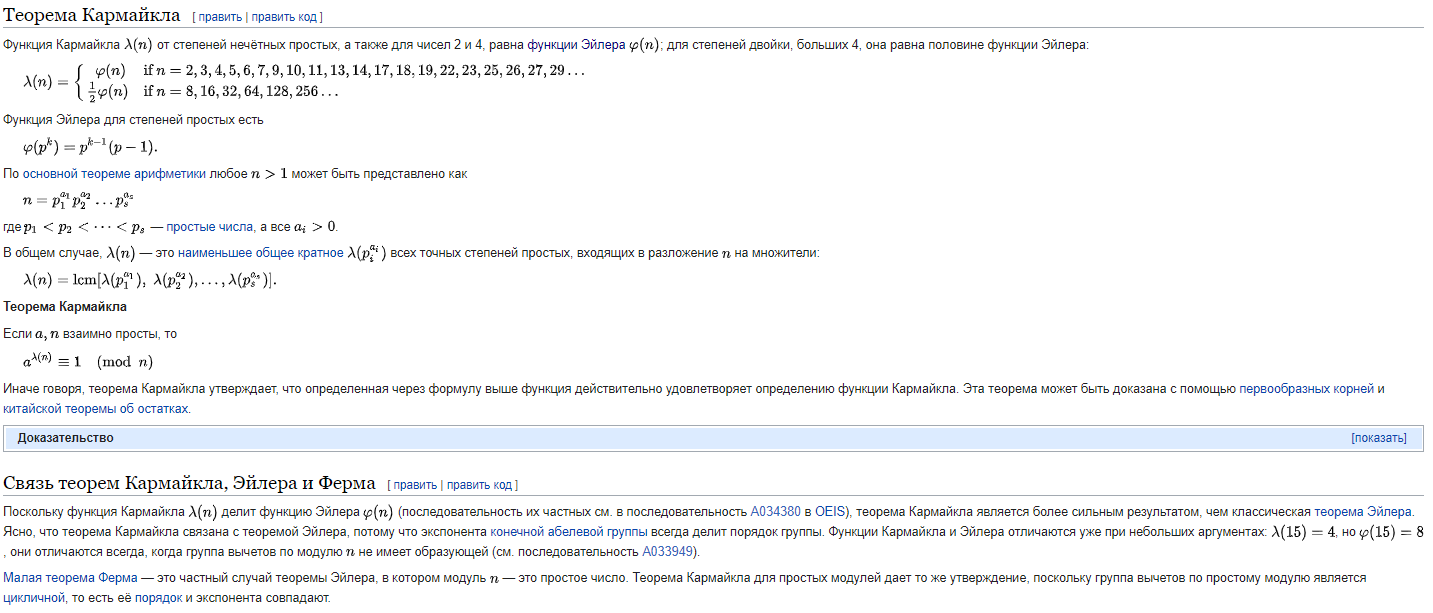
[***https://uk.wikipedia.org/wiki/Функція\_Ейлера***](https://uk.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%8F_%D0%95%D0%B9%D0%BB%D0%B5%D1%80%D0%B0)





[***https://ru.wikipedia.org/wiki/Функция\_Кармайкла***](https://ru.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F_%D0%9A%D0%B0%D1%80%D0%BC%D0%B0%D0%B9%D0%BA%D0%BB%D0%B0)





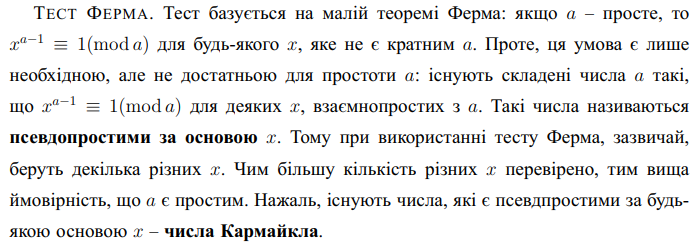
1. ***Тести на простоту Ферма, Соловея-Штрассена та Міллера-Рабіна***

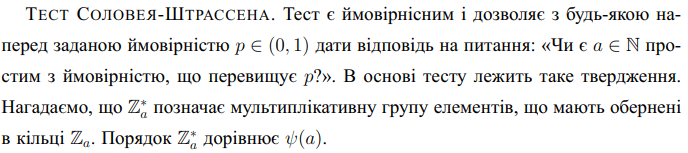
***Тест ферма базується на малій теоремі ферма(якщо а просте то х в степені (а-1) = 1 (mod a)) для будь-якого х що не є кратним для а), це необхідна умова, але не достатня, тому треба перевіряти чи є простим чи складеним число. Тест ферма чітко відповідає чи є число просте і деякі складні числа він може пропустити, наприклад числа Кармайкла. Щоб вирішити цю проблему можна скористатись тестом соловея-штрассена***

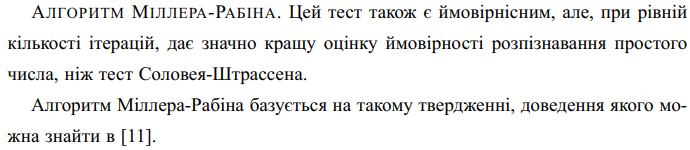
***Тесть соловея-штрассена. Він базується на тому що А в степені (N-1)/2 це символ Якобі, то А в степені -1 це одиниця. Вибирається випадкове число, перевіряється НСД, якщо більше 1 то складене, а якщо = 1 то перевіряється чи це випадкове число(A) в степені (N-1)/2, або чи не дорівнює воно символу Якобі. Якщо не = то число точно складене, тому-що А має бути просте щоб воно було символом Якобі. І знову ж таки перевіряється декілька разів з різними параметрами.***

***Тест міллера-рабіна. Беруть N. N відразу вважається непарним, тому-що якщо воно парне то воно складене відразу, то ми від N віднімаємо 1 і розкладаємо в ступінь двійки помножити на непарне. І шукаємо свідків простоти.***

***Міллера-рабіна більш ефективний ніж Ферма.***

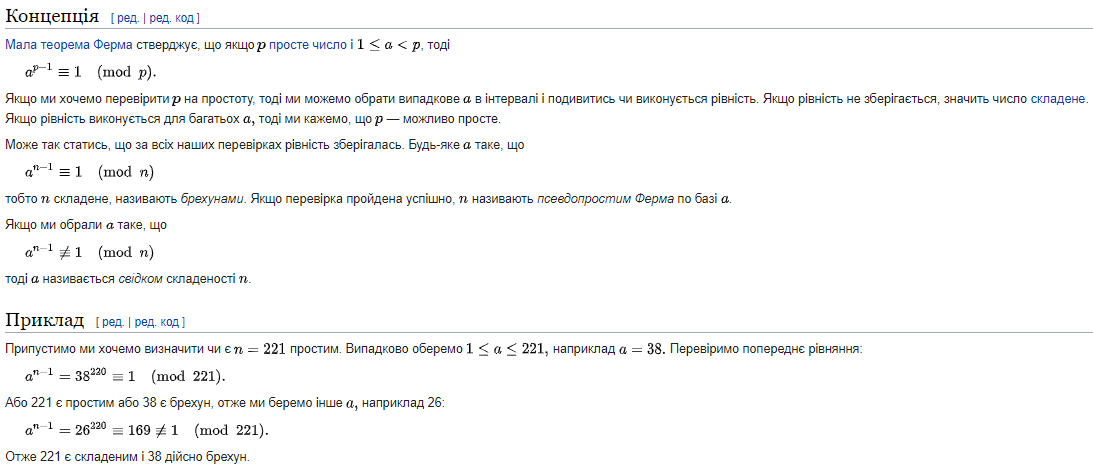




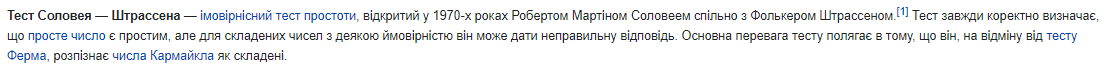


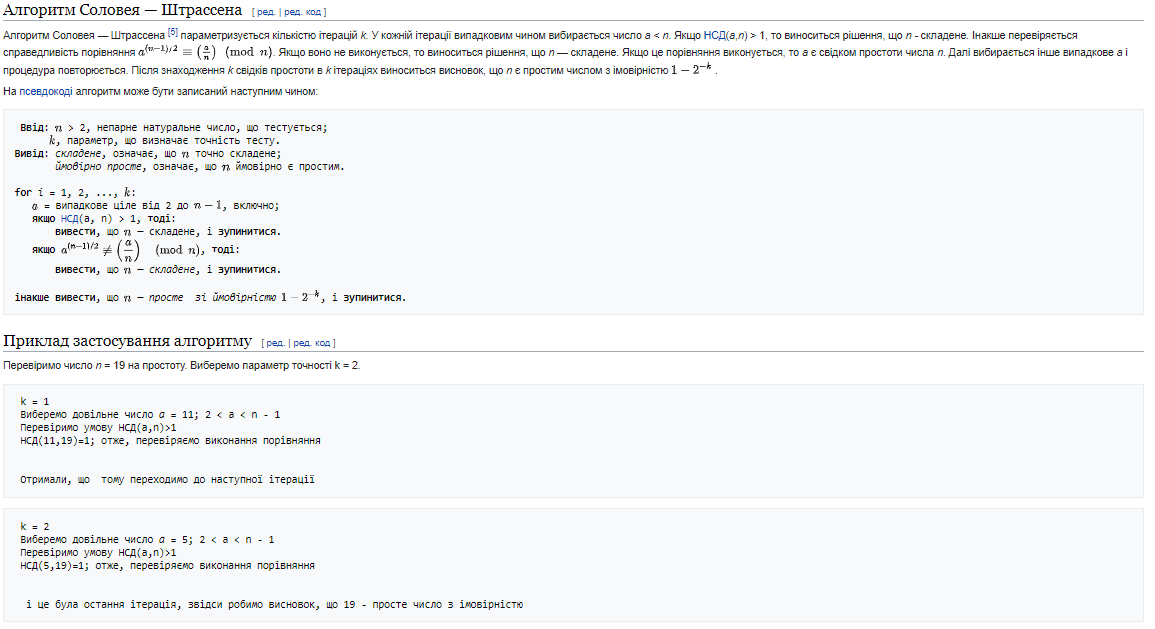
[***https://uk.wikipedia.org/wiki/Тест\_простоти\_Ферма***](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D1%82%D0%B8_%D0%A4%D0%B5%D1%80%D0%BC%D0%B0)

****

****

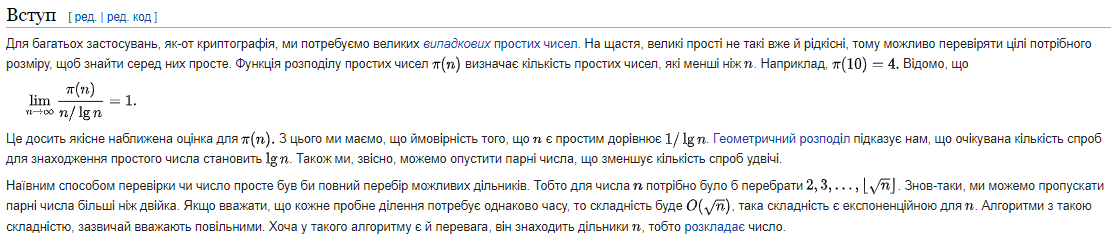
[***https://uk.wikipedia.org/wiki/Тест\_Соловея\_—\_Штрассена***](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%A1%D0%BE%D0%BB%D0%BE%D0%B2%D0%B5%D1%8F_%E2%80%94_%D0%A8%D1%82%D1%80%D0%B0%D1%81%D1%81%D0%B5%D0%BD%D0%B0)

****

****

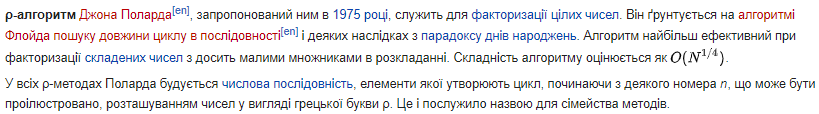
[***https://uk.wikipedia.org/wiki/Тест\_простоти\_Міллера–Рабіна***](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D1%82%D0%B8_%D0%9C%D1%96%D0%BB%D0%BB%D0%B5%D1%80%D0%B0%E2%80%93%D0%A0%D0%B0%D0%B1%D1%96%D0%BD%D0%B0)

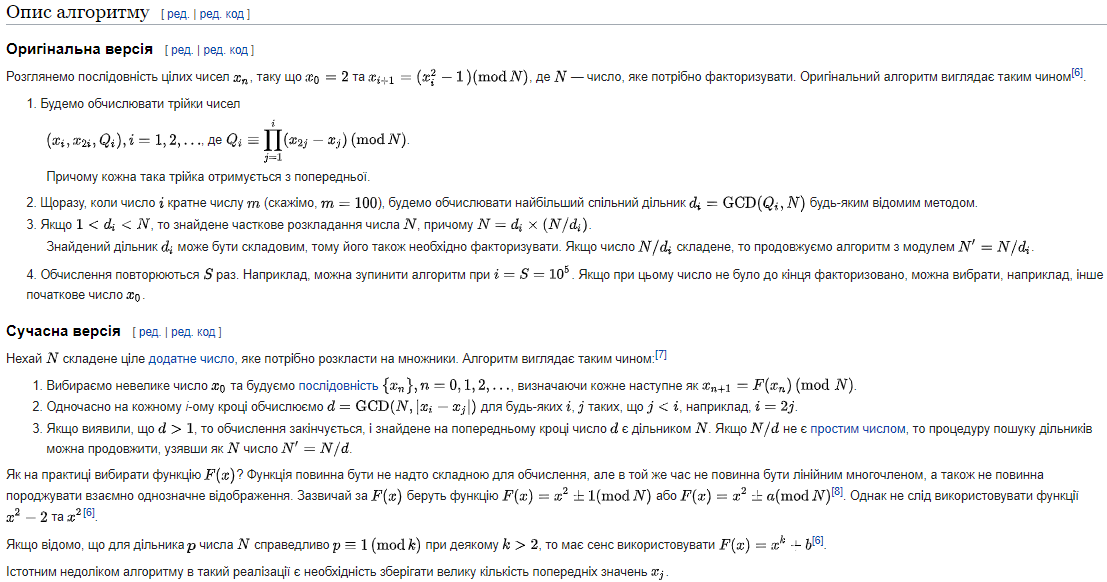
****

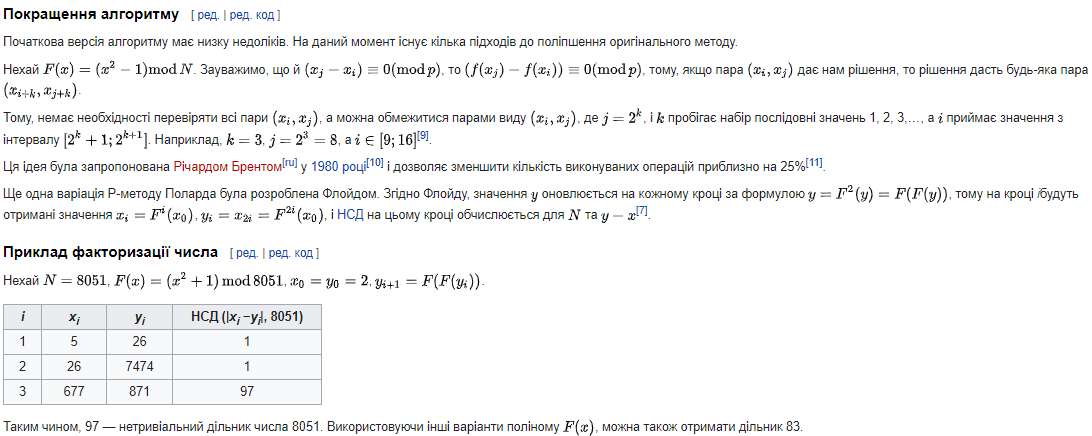
****

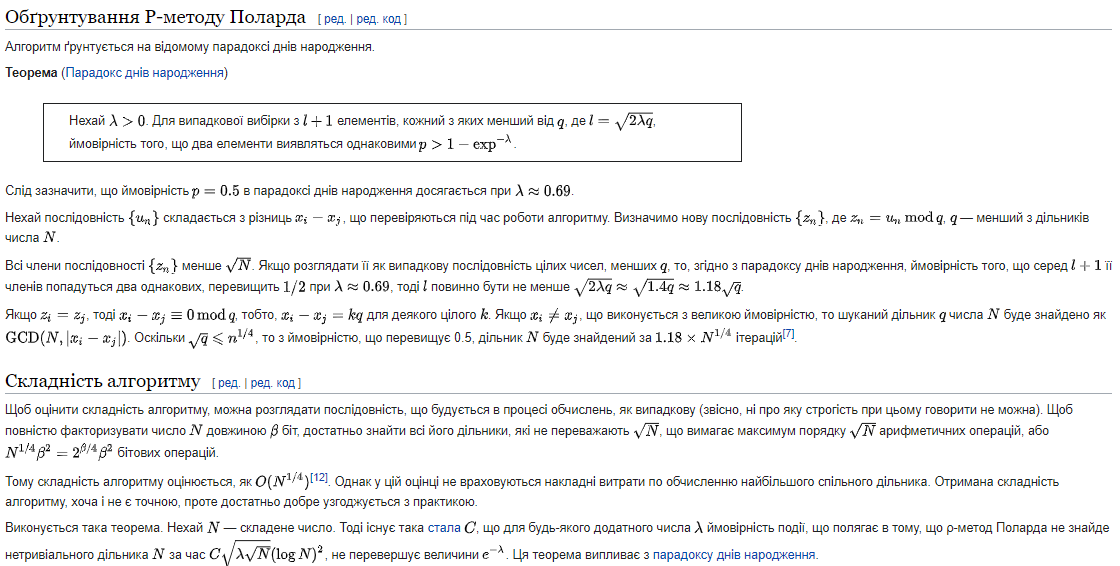
1. ***Алгоритм Полларда розклада складеного числа на множники.***

[***https://uk.wikipedia.org/wiki/P-алгоритм\_Поларда***](https://uk.wikipedia.org/wiki/P-%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%9F%D0%BE%D0%BB%D0%B0%D1%80%D0%B4%D0%B0)

****

****

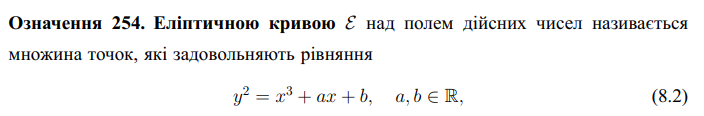
****

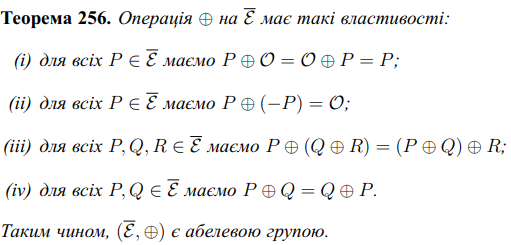


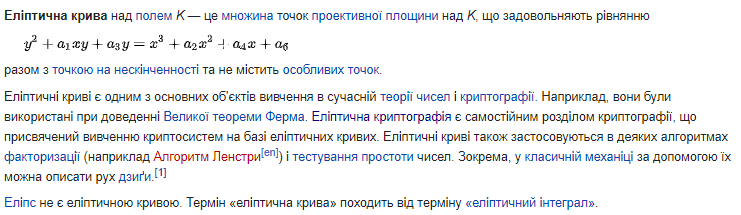
1. ***Рівняння еліптичної кривої. Дискримінант еліптичної кривої. Групова операція на еліптичній кривій. Швидке піднесення у степінь точки на еліптичній кривій.***

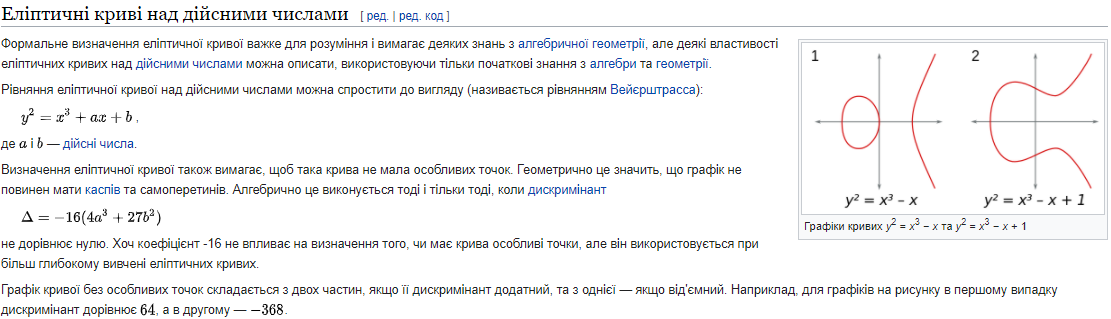
***Дискрімант = -16(4a^3 + 27b^2). Дискрімант прирівнений до нуля це умова того що будуть існувати кратні корені. Якщо дискримінант = 0 то ми не можемо ввести групову операцію (то будуть самоперетини або каски).***

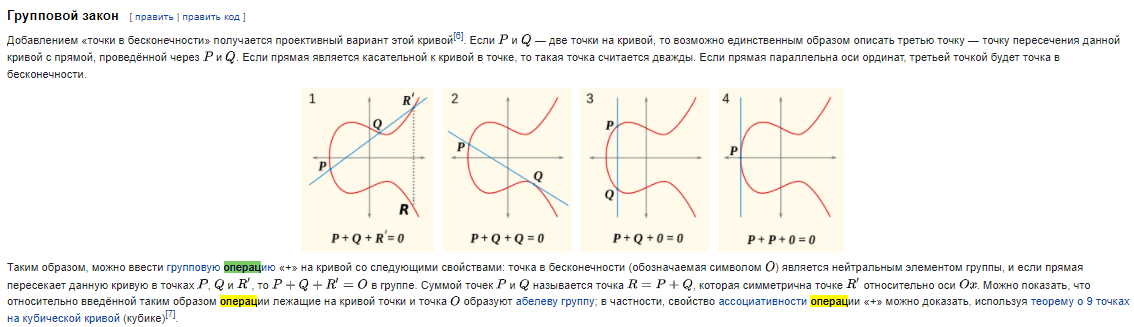
***У нас є точка нескінченності яка є нейтральним елементом. І у нас є якась пряма яка перетиає нашу криву у точках p & q. Пряма перетинається у 3 точках дотику + нейтральному елементі. І тоді p+ q це буде точка симетрична 3 точці яка перетинає.***

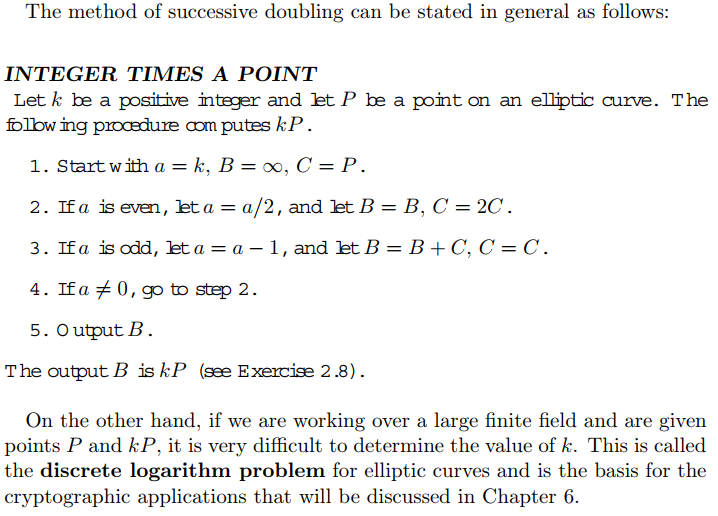








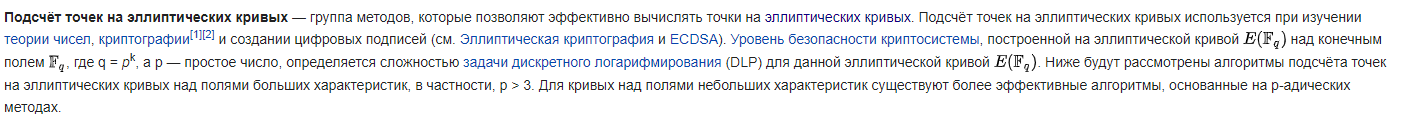




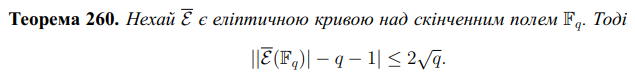
1. ***Кількість точок на еліптичній кривій, теорема Гассе. Медод baby-step giant-step знаходження порядку групи, заданої еліптичною кривою.***

[***https://ru.wikipedia.org/wiki/Подсчёт\_точек\_на\_эллиптических\_кривых***](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B4%D1%81%D1%87%D1%91%D1%82_%D1%82%D0%BE%D1%87%D0%B5%D0%BA_%D0%BD%D0%B0_%D1%8D%D0%BB%D0%BB%D0%B8%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D1%85_%D0%BA%D1%80%D0%B8%D0%B2%D1%8B%D1%85)

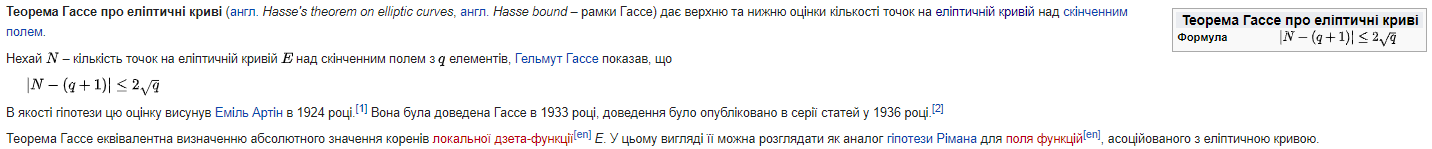
***Якщо є якась еліптична крива нехай ЕПСІЛОН над полем Ф. Тоді за теоремою Гассе, кількість цих точек на полем буде розв’язком нерівності. Нехай ця кількість буде N. |n-q-1| має бути менше за 2 кореня з q. q це кількість елементів поля.***



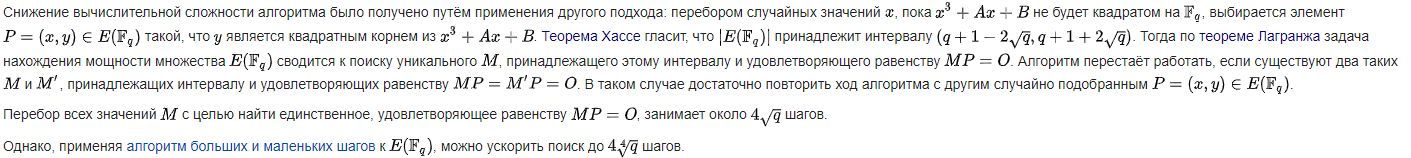


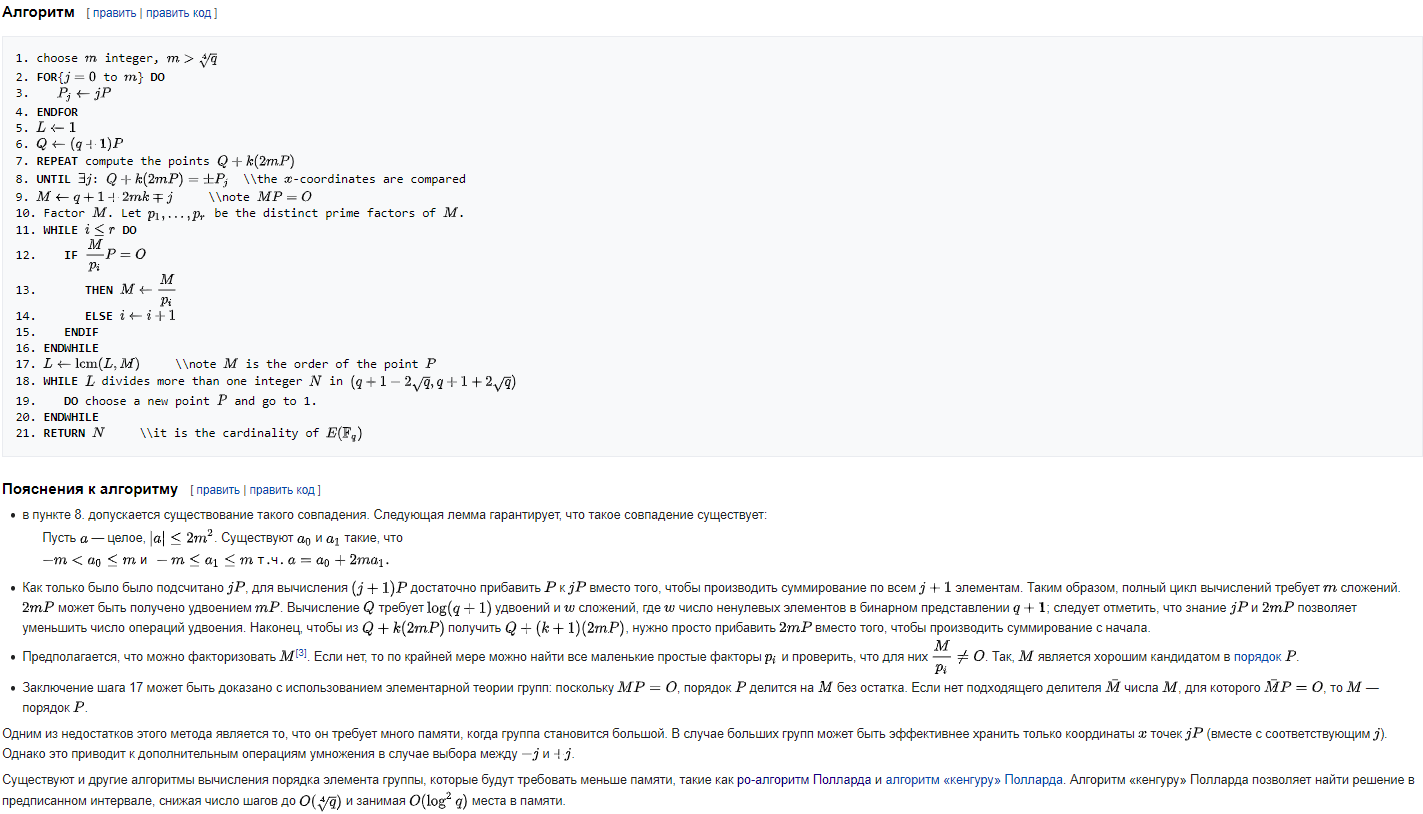


[***https://uk.wikipedia.org/wiki/Теорема\_Гассе\_про\_еліптичні\_криві***](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BE%D1%80%D0%B5%D0%BC%D0%B0_%D0%93%D0%B0%D1%81%D1%81%D0%B5_%D0%BF%D1%80%D0%BE_%D0%B5%D0%BB%D1%96%D0%BF%D1%82%D0%B8%D1%87%D0%BD%D1%96_%D0%BA%D1%80%D0%B8%D0%B2%D1%96)



## Алгоритм больших и маленьких шагов





1. ***Описати як працює шифрування за допомогою еліптичних кривих.***

***Беремо безпечну еліптичну криву для того щоб легко було знайти ключ і представимо що у нас є Аліса, Боб і який посередник між ними. У Аліси та Боба є еліптична крива, проте у кожного є свій секретний ключ. Таким чином Аліса знаходить якусь точку на свій секретний ключ, множить на точку еліптичної кривої. Виходить якась точка ha. Боб робить те ж саме і отримує точку hb. Посередник робить так само. Потім вони обмінюються ключами. Аліса підносять в степінь точку Боба до свій секретний ключ. Боб також підніс до степеню свою точку на ключ Аліси. І в них з’явився суспільний секретний ключ якого немає у посередника. Після цього вони можуть обмінюватись даними за допомогою суспільного секретного ключа.***

[***https://uk.wikipedia.org/wiki/Еліптична\_криптографія***](https://uk.wikipedia.org/wiki/%D0%95%D0%BB%D1%96%D0%BF%D1%82%D0%B8%D1%87%D0%BD%D0%B0_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F)

