Побудова великих простих чисел.

Розглянемо методи перевірки чисел на простоту, при застосуванні яких можна стверджувати, що перевіряючі числа дійсно є простими.

На відміну від попередніх тестів, які використовували необхідні умови простоти й давали відповіді типу ″ - не просте″, або ″не знаю″ або ″імовірність того, що  – не просте, не вище заданого як завгодно малого значення″, дані тести засновані на застосуванні достатніх умов простоти. Тому вони можуть давати як відповіді типу ″ - не просте″, ″не знаю″, так й ″ - просте″.

 Ця властивість застосовується для побудови простих чисел. Загальна схема в цьому випадку така: обирається деяка послідовність чисел спеціального виду, серед яких потрібно знайти просте число, потім до чисел із цієї послідовності застосовується тест доти, доки він не дасть позитивну відповідь.

Якщо ця відповідь ″- не просте″, то обирається наступне число. Якщо отримано відповідь ″ - просте″, то шукане просте число побудоване.

Розглянемо достатні умови простоти чисел, які, звичайно, застосовуються в алгоритмах побудови доказово простих чисел.

*Критерій Люка.*

Теорема, уперше доведена Люка в 1876 р., перетворює малу теорему Ферма в критерій простоти числа , достатня умова якого може бути ефективно використана для доказу простоти цього числа.

***Теорема 1.*** *(Люка)*

Натуральне число є простим у тому і тільки в тому випадку, коли виконується умова

** (1)

*Доведення.*

Якщо  просте, то в полі  є примітивний елемент, що і буде шуканим. Навпаки, нехай для елемента  виконується умова (1). Якщо , те, причому умова (1) гарантує, що . Отже,  і
 – просте. Теорема доведена.

*Зауваження* (Селфридж).

Умова (1) у даній теоремі можна замінити на кожну з таких умов:

** (2)

** (3)

Дійсно, те, що (1) =>(2) й (1)=>(3) , очевидно.

Доведемо, що (3)=>(2) . Нехай . За умовою для кожного  знайдеться  таке, що , але  не ділить число .

Отже, . Отже, знайдуться елементи , такі, що . Тепер елемент  буде шуканим, тому що порядки елементів  взаємно прості й

******

Теорема Люка дозволяє довести простоту числа  у випадку, коли відоме розкладання на прості співмножники числа 

Для цього можна використати детермінований алгоритм, заснований на переборі всіх можливих значень , або скористатися таким імовірнісним методом:

1. обираємо випадкові числа  й перевіряємо для них умову (1);
2. якщо умова (1) виконана хоча б для одного із цих чисел, то  просте, якщо ні, то відповідь невідома.

Аналогічний метод можна побудувати, використовуючи умову (3).

Проілюструємо цей метод стосовно до чисел Ферма.

Числами Ферма називають числа виду (Покажіть, що число виду  може бути простим у тому і тільки в тому випадку, коли .)

Ферма висловлював припущення, що всі числа такого виду – прості. При  це дійсно так. Але при , як показав Ейлер в 1732 р., справедливе розкладання

.

В 1878р. Іван Михейович Первушин показав, що числа  й  також не є простими. (Зазаначимо, що число  має 2525223 цифри. При відтворенні такого числа знадобився б рядок довжиною в 5 км або книга об'ємом 1000 сторінок).

***Теорема******2****.* (*Пепін, 1877*).

Числа при  є простими в тому і тільки в тому випадку, коли виконується умова 

*Доведення.* Оскільки єдиним простим дільником число  є 2 , то достатньо перевірити умову теореми Люка при . Покажемо, що як число  можна взяти число 3, тобто достатньо перевірити умову  Використовуючи формулу Ейлера для обчислення значень квадратичних лишків і квадратичний закон взаємності Гаусса отримуємо, що при простому  має бути



Тепер зазаначимо, що , і тому умова  рівносильна рівності Теорема доведена.

Теорема Люка послужила відправним пунктом для побудови цілої групи тестів, що дозволяють перевіряти простоту числа. Багато хто з них отримали назву - методів, тому що припускають знання повної або часткової факторизації числа .

Ще одне узагальнення теореми Люка засновано на розгляді інших груп замість мультиплікативної групи . Фактично, доказ простоти числа  в теоремі Люка засновано на вивченні властивостей групи : якщо будь-яким чином вдається встановити, що її порядок дорівнює , то число  – просте.

Дана ідея лежить в основі таких методів, як метод еліптичних кривих і метод числового поля.

***Теорема Поклінгтона.***

В 1914 р., Х. Поклінгтоном була доведена наступна теорема.

***Теорема 3.*** *(Поклінгтон).*Нехай , де  – просте, що не є дільником . Якщо існує ціле  таке, що  й , то кожен простий дільник  числа  має вигляд  при якомусь .

*Доведення.* Нехай  – простий дільник числа . Тоді з умови теореми
випливає, що  й . Звідси отримуємо, що порядок  елемента  за модулем  задовольняє умови:  і  не ділить . Тому . У силу малої теореми Ферма . Отже, . Теорему доведено.

Застосовуючи дану теорему для всіх дільників  числа , отримуємо наступну теорему, що є узагальненням теореми Люка на випадок .

***Теорема 4.*** Нехай , де . Якщо для будь-якого простого дільника  числа  існує ціле  таке, що  й , тоді число -просте.

*Доведення.* Нехай  – складене й – нетривіальний простий дільник числа . Зазначимо, що завжди можна вибрати дільник так, що . Тоді з умови теореми випливає, що для всіх простих дільників  числа  існує ціле  таке, що  й .

Міркуючи аналогічно зауваженню до теореми Люка, отримуємо, що має знайтися елемент, який має порядок рівний  за модулем . У силу малої теореми Ферма . Отже, справедливий ланцюжок нерівностей

.

Але , протиріччя.

Дана теорема показує, що якщо вдалося частково факторизувати число , причому факторизована частина задовольняє умову , то  – просте.

Перш ніж переходити до подальшого, приведемо дві класичні частки випадку даної теореми.

***Теорема 5.*** *(Прот, 1878).* Нехай , де .

Якщо існує число , для якого виконується умова

,

то – просте.

***Теорема 6.*** *(Прот, 1878).* Нехай , де ,  і 3 не ділить . Тоді  просте в тому і тільки в тому випадку, коли виконується умова

.

*Доведення.* У силу теореми Поклінгтона достатньо перевірити умову  при  й . Оскільки за умовою , то умова  рівносильна виконанню рівності



Зазаначимо, що якщо в теоремі Поклінгтона замінити рівність  на більш слабку умову, то можна отримати
наступний результат.

***Лема 1.*** Нехай , де  – просте число, що не є дільником. Якщо існує ціле  таке, що  й , то знайдеться простий дільник  числа  виду  при якомусь .

*Доведення.* Нехай . Тоді за умовою теореми в силу китайської теореми про залишки випливає, що існує таке , що  й. Звідси отримуємо, що порядок  елемента за модулем  задовольняє умови: і  не ділить. Тому.

У силу леми Гаусса про циклічність мультиплікативної групи кільця  одержуємо. Зазначимо, що числа  й  взаємно прості як дільники сусідніх чисел. Тому. Отже,.

Хоча цей результат слабкіше, ніж теорема Поклінгтона, даний підхід, як показав Н. Дієметко в 1988 р., також може бути ефективно використаний для доведення простоти чисел.

***Теорема*** *(Дієметко).* Нехай , де  – просте, – парне й  Якщо існує ціле  таке, що  й  , то  – просте.

*Доведення.* Нехай  – не просте й . Тоді за лемою отримуємо, що існує таке , що.

Позначимо  Тоді , де  й . Звідси . Отже, , де  – не може дорівнювати 0, інакше  – просте, або 1, тому що  – непарне. Аналогічно,. Таким чином,

.

Протиріччя. Теорему доведено.

Зазаначимо, що за умовою теореми числа  й  можуть бути не взаємно прості. Ця теорема лежить в основі алгоритму генерації простих чисел у вітчизняному стандарті на цифровий підпис Р 34.10-94.

У ньому як  обираються не дуже високі степені числа 2, а  перебуває перебором. (З 1 липня 2002 р. цей стандарт був замінений на новий Р 34.10-2001).

***Метод Маурера***

В 1995 р. У. Маурер опублікував швидкий алгоритм генерації доведених простих чисел, близьких до випадкового. У його основі лежить посилення теореми Поклінгтона на випадок, коли факторизована частина  числа  задовольняє нерівності . Крім того, йому вдалося оцінити ймовірність успіху при випадковому пошуку числа  в умові теореми Поклінгтона.

Наступна лема є спеціальним випадком теореми Поклінгтона.

***Лема 2.*** Нехай  Якщо існує ціле  таке, що для будь-якого простого дільника  числа  виконані умови  і , те кожен простий дільник  числа  має вигляд  при деякому цілому  Якщо, крім того,  або  – парне й , то  – просте.

*Доведення.* Нехай  – складене й  – нетривіальний простий дільник числа . Тоді за умови теореми випливає, що  й  . Міркуючи аналогічно зауваженню до теореми Люка, отримуємо, що має знайтися елемент, який має порядок рівний  за модулем . У силу малої теореми Ферма .

Для доведення другого твердження, припустимо, що . Тоді .
Якщо , то  Якщо  - непарне й , то  й



просте число поклінгтон мауер люк

Протиріччя.

Наступна лема доведена Д. Коувером і Дж. Куіскуотером в 1992 р.

***Лема 3.*** Нехай  і  задовольняють умову леми 1. Визначимо числа  й  рівністю . Якщо  й число  не дорівнює нулю й не є повним квадратом, то  - прості.

*Доведення.* Відповідно до леми 1 для кожного простого дільника  числа  виконується нерівність  За умовою . Тому, якщо число

 – складене, то воно не може мати більше двох простих дільників. Нехай

 и. .

Маємо  інакше .

Якщо  , то 

Звідси , однак у цьому випадку  Тому .

Отже,  і . За теоремою Вієта  є коренями квадратного рівняння , що має розв’язання в цілих числах у тому і тільки в тому випадку, якщо  є повним квадратом або нулем. Лему доведено.

Зазначимо, що переконатися, що задане число не є повним квадратом, можна, обчисливши символ Лежандра для декількох маленьких простих модулів. Якщо при деякому модулі число не буде квадратичним відрахуванням, то воно не буде й повним квадратом.

Нехай  – функція Ейлера.

***Лема 4.*** Нехай  – просте число й . Позначимо через  число елементів , порядок яких ділиться на . Тоді справедлива оцінка

,

причому рівність виконується в тому й у тільки в тому випадку, коли 

*Доведення.* Використовуючи властивості функції Ейлера, отримуємо



причому рівність виконана в тому і тільки в тому випадку, коли

