Алгоритм побудови великого простого числа. Найефективніший спосіб побудови простих чисел випливає з дещо модифікованої малої теореми Ферма.

Теорема 37. *Нехай n,s – непарні натуральні числа і $n-1 = r \cdot s$, причому для кожного простого дільника q числа s існує ціле число a таке, що*

$$a^{n-1} \equiv 1\ (mod\ n), \quad \text{НСД}(a^{\frac{n-1}{q}} - 1, n) = 1. \tag{2.17}$$

Тоді кожний простий дільник числа n задовольняє конгруенції $p \equiv 1\ (mod\ 2s)$.

Доведення. Нехай p – простий дільник числа n, а q – деякий дільник числа s. З умови (2.17) випливає, що в полі лишків F_p мають місце співвідношення

$$a^{n-1} = 1,\ a^{\frac{n-1}{q}} = 1,\ a^{p-1} = 1. \tag{2.18}$$

Нехай r означає порядок елемента a в мультиплікативній групі поля F_p. Перші два співвідношення із (2.18) означають, що q входить в розклад на прості множники числа r в такому ж степені, як і в розклад числа $n-1$, а це означає що $p-1$ ділиться на r. Отже, кожний простий дільник числа s входить в розклад числа $p-1$ в степені не меншому, ніж в s, так що $p-1$ ділиться на s. Крім того, $p-1$ парне. ■

Наслідок 4. *Якщо умови теореми 37 виконані і* $r \le 4s+2$, *то число* n *– просте.*

Дійсно, нехай n дорівнює добутку не менше двох простих чисел. Кожне з цих чисел на підставі теореми 37 не менше, ніж $2s+1$. Але тоді $(2s+1)^2 \le n = sr+1 \le 4s^2+2s+1$, а це суперечить нерівності $(2s+1)^2 \le 4s^2+2s+1$. ■

Опишемо тепер спосіб, як за допомогою останнього твердження, маючи просте число s, можна побудувати суттєво більше просте число n.

Виберемо випадковим чином парне число r з проміжку $s \le r \le$ $\le 4s+2$ і покладемо $n = sr+1$. Перевіримо число n на відсутність малих простих дільників, поділивши його на ці прості числа. Виконаємо цю перевірку декілька разів за допомогою алгоритму тестування непростоти числа. Якщо при цьому виявиться, що n складене, то вибираємо нове число r і знову повторюємо обчислення. Так діємо до тих пір, доки не буде знайдене число n, яке витримало випробування алгоритмом достатню кількість разів. В цьому випадку появляється надія на те, що n – просте число і цю простоту потрібно довести тестами теореми 37.

З цією метою випадковим чином вибираємо число a, $1 < a < n$, і перевіряємо для нього виконання співвідношень

$$a^{n-1} \equiv 1 \ (mod\ n), \quad \text{НСД}(a^r-1, n) = 1. \tag{2.19}$$

Якщо ці співвідношення виконуються для вибраного a, то на підставі наслідка 4 можна стверджувати, що число n просте. Якщо ж ці співвідношення не виконуються, то вибираємо інше число a і повторюємо ці дії доти, доки таке число не буде знайдено.

Припустимо, що побудоване число n дійсно просте. Скільки разів прийдеться повторювати вибір числа a, доки не буде знайдено таке, для якого виконуються умови (2.19)? Зауважимо, що для простого числа n перша умова (2.19) на підставі малої теореми Ферма виконуватиметься завжди. Числа a, для яких не виконується друга умова (2.19), задовольняють конгруенції $a^r \equiv 1 \ (mod\ n)$. А ця конгруенція в полі F_n, як відомо має не більше ніж r розв'язків. Один з цих розв'язків $x = 1$. Тому на інтервалі $1 < a < n$ буде не більше $r - 1$ чисел, які задовольняють умови (2.19). А це означає, що вибираючи випадковим чином число a з проміжку $1 < a < n$ при простому n можна знайти з ймовірністю більшою ніж $1 - O(s^{-1})$ число a, для якого виконуються умови (2.19) теореми 37 і тим самим довести, що n дійсно просте число.

Отримане таким чином просте число n буде задовольняти нерівність $n > s^2$, тобто буде записуватися з вдвічі більшою кількістю цифр, ніж число s. Замінивши в цьому процесі число s числом n і повторивши всі вищеописані дії з числом n, можна побудувати ще більше просте число. Якщо починати пошук з 10-розрядного числа (а його простоту можна легко перевірити шляхом ділення на табличні малі прості числа) і повторити описаний процес достатню кількість разів, то можна побудувати просте число потрібної величини.

Теоретичні підстави описаного процесу ґрунтуються на дослідженнях розподілу простих чисел в арифметичній прогресії $2sn+1$, де $n = 1, 2, \ldots$. В цій прогресії, як показав Діріхлє в 1839 році, знаходиться нескінченно багато простих чисел. Нас цікавлять числа, які знаходяться недалеко від початку цієї прогресії. Відповідь на це питання було отримано Люстерніком в 1944 році, який показав, що найменше просте число в цій прогресії не перевищує величини s^c, де c – досить велика константа.

Досвід обчислень на комп'ютерах показує, що прості числа в арифметичній прогресії зустрічаються досить близько від її початку і розміщені досить щільно. Існує гіпотеза Крамера, що відстань між сусідніми простими числами p_n і p_{n+1} в натуральному ряді чисел має оцінку $p_{n+1} - p_n = O(\ln^2 p_n)$, яка підтверджується й іншими результатами.