ПІДСЕКЦІЯ ІНФОРМАТИКИ ТА КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

ЕФЕКТИВНИЙ АЛГОРИТМ РОЗПІЗНАВАННЯ ДЕЯКОЇ ПІДМНОЖИНИ СКЛАДНИХ ЧИСЕЛ

І. Кравченко (кафедра інформатики НаУКМА)

Для багатьох задач математики, які мають практичне застосування, на сьогодні ще не знайдено ефективних алгоритмів їх розв'язку. В класі **NP** (Nondeterministically Polinomial) всіх перебірних задач визначені підмножини задач, які мають поліноміальний алгоритм розв'язку (клас **P**) та найбільш складні задачі - **NP**-повні задачі (**NPC**). Основна проблема теорії складності - **NP=P**? Якщо ці класи не рівні, то для **NP**-повних задач не існують ефективні (поліноміальні) алгоритми.

Існують задачі, які належать до проміжного шару (на сучасному етапі) - тобто задачі, для яких не знайдено поліноміального алгоритму і не доведено їх **NP**-повноту. З того, що класи **P** та **NP** не рівні, не можна буде зробити висновок, що для цих задач не існує ефективного алгоритму.

Такою є задача розпізнавання складних чисел (або простих чисел). Всім строгим у математичному сенсі методам необхідно такого самого порядку елементарних арифметичних операцій, як і величина числа, що тестується. Існують методи, які ефективно вирішують задачу при істинності деякої гіпотези (гіпотези Рімана) або дають відповідь з деякою ймовірністю. Можливо, складнішою є задача знаходження простих дільників натурального числа. Складність цієї задачі є основою декількох схем криптографічного захисту інформації.

Вся множина непарних натуральних чисел з точки зору структури періодичної частини послідовності Фібоначчі по модулю натуральних чисел розбивається на чотири рівнопотужні підмножини, одну з яких утворюють тільки складні числа. На основі цього ми пропонуємо ефективний алгоритм розпізнавання належності числа до даної підмножини, який можна використовувати для знаходження нетривіальних множників складних чисел спеціальних видів. Складність алгоритму має лінійну оцінку від подвійного запису тестованого числа.