Cryptography.7. http://www.secg.org/download/aid-780/sec1-v2.pdf *2009 p.8. Глухов В.С., Еліас Р. Виявлення помилок признаходженні оберненого елемента в Гауссівському нормальному базисі типу 2 Полів Галуа GF(2^m) // Радіоелектронні і комп'ютерні системи. – 2010. – № 6(47). – С. 129–133. 9. Мельник А., Морозов Ю., Мельник В., Коркішко Т. Проблеми і тенденції розвитку апаратних засобів захисту інформації// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ. – 2002. – Вип. 5. – С. 168–162. 10. Коркішко Т., Мельник А. Стан та напрямки розвитку надвеликих інтегрованих схем захисту інформації // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ. – 2000. – С. 275 – 281. 11. Глухов В.С. Порівняння поліноміального та нормального базисів представлення елементів полів Галуа // Вісник Національного університету "Львівська політехніка". – 2007. – С. 22–27. 12. MuthuKumar B., Jeevananthan S. Performance Enhanced Co-Processor for Elliptic Curve Cryptography over GF (p) European Journal of Scientific Research ,ISSN 1450-216X Vol.68 No.4 (2012), pp. 544-555. 13. Recommendation for Key Management // Special Publication 800-56 Part 1 Rev. 3,* NIST*, 05/2007 14. Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, PKC2000: p. 446-465, 01/2000.15. Handbook of Information Security, Arjen K. Lenstra, 06/2004. 17.Yearly Report on Algorithms and Keysizes (2011), D.SPA.16 Rev. 1.0, ICT-2007-216676 ECRYPT II, 06/2011. 17. Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 3, NIST, 05/2011. 18. Mécanismes cryptographiques - Règles et recommandations, Rev. 1.20, FNISA , 01/2010.19. Algorithms for Qualified Electronic Signatures, BNetzA, BSI, 05/2011.*

УДК 681.3

С.В. Івасьєв
Інститут мікропроцесорних систем керування об'єктами електроенергетики
Карпатського державного центру інформаційних засобів і технологій
Національної академії наук України

МЕТОД ФАКТОРИЗАЦІЇ ВЕЛИКОРОЗРЯДНИХ ЧИСЕЛ У БАЗИСІ РАДЕМАХЕРА

Подано теоретичні основи та метод факторизації великорозрядних чисел Мерсена, проаналізовано основні властивості та розподіл чисел Мерсена. Наведено метод факторизації Ферма. Розроблено алгоритм факторизації великорозрядних чисел Мерсена та алгоритм знаходження залишку в базисі Радемахера.

Ключові слова: метод факторизації, великорозрядні числа Мерсена, базис Радемахера.

The paper presents the theoretical basis and method for factorization large-digit numbers Mersen, analyzed the basic properties of numbers and distribution Mersen numbers. The method of factorization Farm. An algorithm for factoring big Mersen numbers and algorithm for finding balance in the basis of Rademacher was created.

Key words: method for factorization, large-digit numbers Mersen, basis Rademacher.

Вступ

Важливим завданням опрацювання інформаційних потоків у комп'ютерних системах є розроблення нових методів та алгоритмів виконання операцій з великорозрядними числами (ВРЧ) [1], які широко використовуються в системах захисту інформаційних потоків. Найвідоміша реалізація алгоритму шифрування RSA, Ель–Гамаля, а також електронного цифрового підпису [1] ґрунтується на алгоритмічній складності задачі факторизації чисел. Відомі алгоритми факторизації ВРЧ характеризуються великою обчислювальною складністю. Тому задачі криптографії систем захисту, основані на використанні цих методів та тестів простоти для великих параметрів крипто-перетворень, стають практично нездійсненними.

Одним з перспективних напрямів розв'язання задач факторизації ВРЧ є застосування теоретико-числового базису (ТЧБ) Радемахера [1], оскільки в класичній теорії використовується тільки десяткова система числення, яка має обмежені обчислювальні властивості й характеризується експоненційною обчислювальною складністю.

Огляд літератури

Теорія чисел, яка є основою криптографічних алгоритмів, а також багатьох методів опрацювання інформації, зародилась ще 100 р. д.н.е. в Китаї. Продовжили її розвиток і створили основу такі видатні вчені, як Евклід, Діофант, Ератосфен, Ейлер, Ферма, Декарт, Гільберт, Лежандр, Матіясевич, Адамар, Сельберг, Ріман, Гаусс, Якобі, Мінковський, Рамануджан та інші [1, 2].

На особливу увагу заслуговують тести простоти числа, які активно використовуються в криптосистемах. Найпоширенішими з них є: тести, основані на теоремах Вільсона та Ферма, тест Міллера – Рабіна, Соловея – Штрассена, Люка – Лемера, Пепіна, Прота, Агравала-Каяла-Саксени, а також тест Бейлі-Померанса-Селфриджа, Вагстафа [1].

Значний внесок у розвиток теорії та застосування в галузі обчислювальних машин у різних ТЧБ зробили І.Й. Акушський, Д.І. Юдицький, Е.И. Брюхович, Я.М. Николайчук та інші [1,3].

У [4] наведено основні результати пошуку чисел Мерсена та дослідження щодо факторизації чисел. Останнє число, яке знайшов учасник проекту GIMPS з Норвегії 12 квітня 2009 року, є 47-м в послідовності відкриття, але за значенням воно поступається попередньому відомому. Це число дорівнює $2^{42643801}$-1 і складається з 12 837 064 десяткових знаків, порядковий номер знайденого числа Мерсена не встановлено, оскільки факторизацію проведено за допомогою імовірнісних алгоритмів перевірки на простоту [4].

У таблиці наведено значення простих чисел Мерсена, включаючи їх порядковий номер та кількість цифр у десятковому представленні.

Прості числа Мерсена

Номер числа Мерсена	1-39	40	41	не встановлено	не встановлено	не встановлено	не встановлено	не встановлено	не встановлено
Експонента n	2-13466917	20996011	24036583	25964951	30402457	32582657	37156667	42643801	43112609
Кількість цифр	1-4053946	6320430	7235733	7816230	9152052	9808358	11185272	12837064	12978189

Оскільки алгоритм пошуку простих чисел Мерсена є ймовірнісним, то порядкові номери останніх шести чисел не встановлено, а їхня кількість в інтервалі від $2^{25964951}$-1 до $2^{43112609}$-1 може змінитись.

Актуальність розроблення алгоритмів опрацювання великорозрядних чисел

Разом з виникненням у криптографії нових понять і методів розширилося і коло криптографічних додатків теорії чисел. Для елементарної та аналітичної теорії чисел все ширше використовується алгебраїчна теорія чисел (тести на простоту із застосуванням сум Гаусса і Якобі, криптосистеми, основані на квадратичних полях, решето числового поля) і аналітична геометрія (факторизація за допомогою еліптичних кривих, криптосистеми, основані на еліптичних і гіпереліптичних кривих і абелевих групах). У наш час широко використовується алгоритм з квадратичним решетом числового поля, що є трудомістким і має експоненційну складність[1].

Нині існує гостра потреба виконувати обчислення з ВРЧ [2], а саме генерування випадкових простих та взаємно простих ВРЧ, операції модулярного множення та експоненціювання, пошуку залишку чисел тощо.

Мета роботи

Мета роботи полягає у розробленні алгоритму факторизації чисел Мерсена в ТЧБ Радемахера та дослідженні його роботи.

Властивості чисел Мерсена

Теорема Люка–Лем'єра показує, що для деякого натурального n значення $2^n - 1$ є простим, тоді n також є простим [2]. Отже, ця теорема суттєво зменшує діапазон пошуку чисел Мерсена, оскільки перебір здійснюється відповідно до простих значень експоненти n. Для факторизації ВРЧ необхідно надзвичайно багато обчислювальних ресурсів, тому аналіз та дослідження можливих простих експонент досить важливі. На рис. 1 показано послідовність розподілу простих експонент чисел Мерсена на логарифмічній шкалі.

Рис. 1. Розподіл простих експонент чисел

Аналіз графічних результатів (рис. 1) показує, що розподіл простих експонент у числах Мерсена має певну залежність. З урахуванням апроксимації результатів досліджень, які мають залежність, близьку до лінійної, можна оцінити значення наступної експоненти простого числа.

На основі проведених досліджень простих експонент чисел Мерсена можна виділити діапазон чисел, серед яких міститиметься наступне число Мерсена. Очевидно, що наступні прості числа Мерсена в результаті спостережуваної апроксимації будуть в інтервалі від $2^{43112609}$ до $2^{48122608}$.

Алгоритм знаходження залишку в базисі Радемахера

Однією з важливих операцій під час дослідження чисел Мерсена є факторизація та знаходження залишків за простими модулями.

Класичні алгоритми пошуку залишку ґрунтуються на використанні багаторозрядного базису Радемахера, який має певні недоліки та функціональні обмеження [5]. Загальний недолік розглянутих у [5] структурних схем пошуку залишків – отримання не завжди найменших залишків, а також надлишковість порівнянь. Тому доцільне розроблення нового методу, який базується на застосуванні особливостей чисел Мерсена в ТЧБ Радемахера [6].

Основними перевагами цього алгоритму є зменшення надлишкового використання пам'яті та кількості порівнянь. Це дозволяє зменшити обчислювальну складність на 1–2 порядки [6].

Особливістю такого алгоритму є використання базису Радемахера й обмеженої кількості операцій додавання [6].

Зазначимо, що запропонований алгоритм універсальний і може використовуватись для знаходження складених чисел.

На рис. 2 подано блок-схему алгоритму пошуку залишків великорозрядних чисел Мерсена за простими модулями.

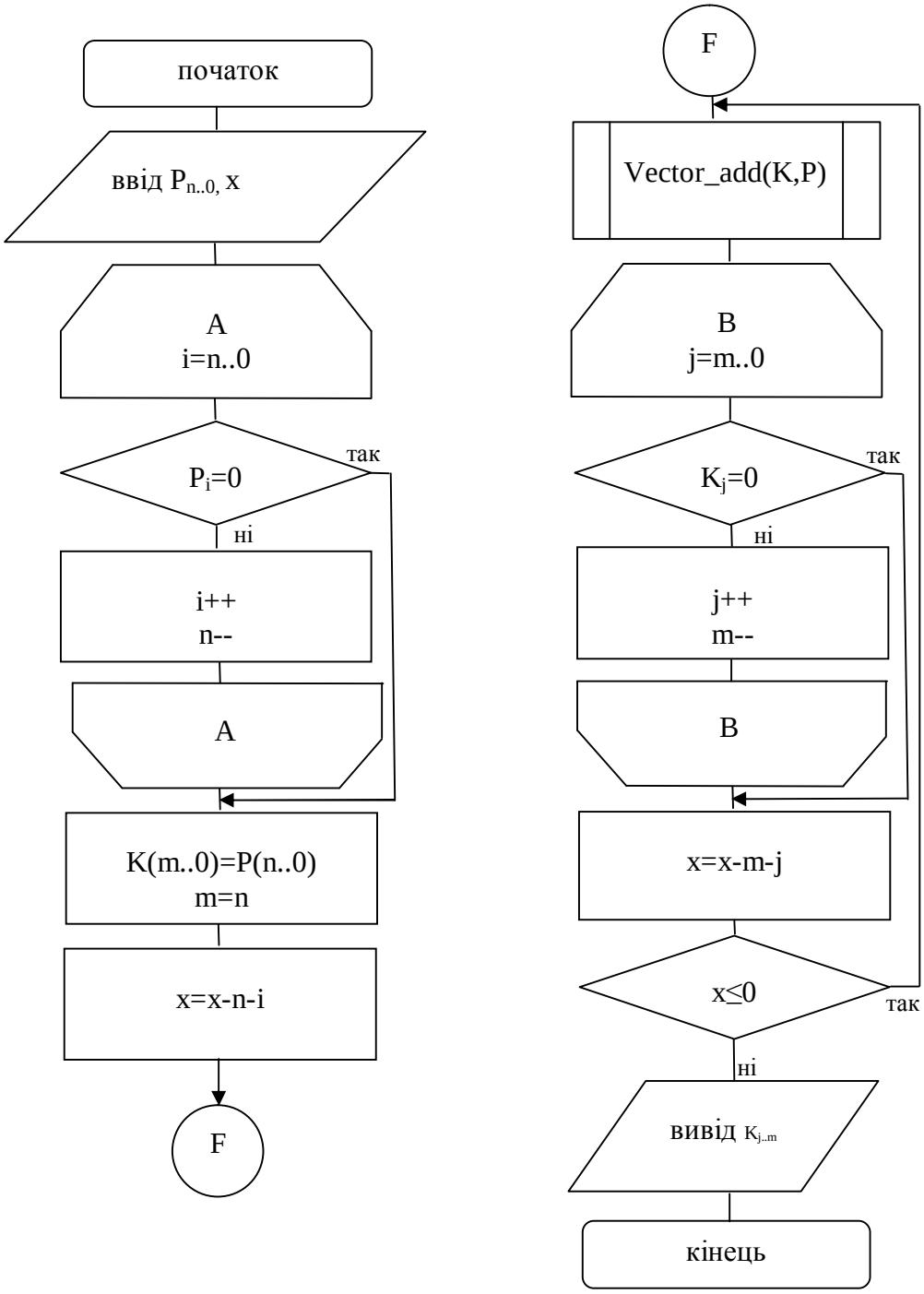

Рис. 2. Блок-схема алгоритму пошуку залишків ВРЧ Мерсена за простими модулями

Як свідчить отримана аналітика часової складності запропонованого методу, цей метод характеризується більшою швидкодією порівняно з класичними.

Алгоритм факторизації ВРЧ Мерсена

Для наочності порівняння алгоритмів наведемо на рис. 3 блок-схему алгоритму факторизації ВРЧ Мерсена прямим перебором [4].

Складність алгоритму факторизації прямим перебором оцінюється обчислювальною складністю $\Theta(N^{1/2})$ [1], де N – число, яке факторизують. Це означає, що обчислювальна складність залежить від розрядності числа, яке факторизують.

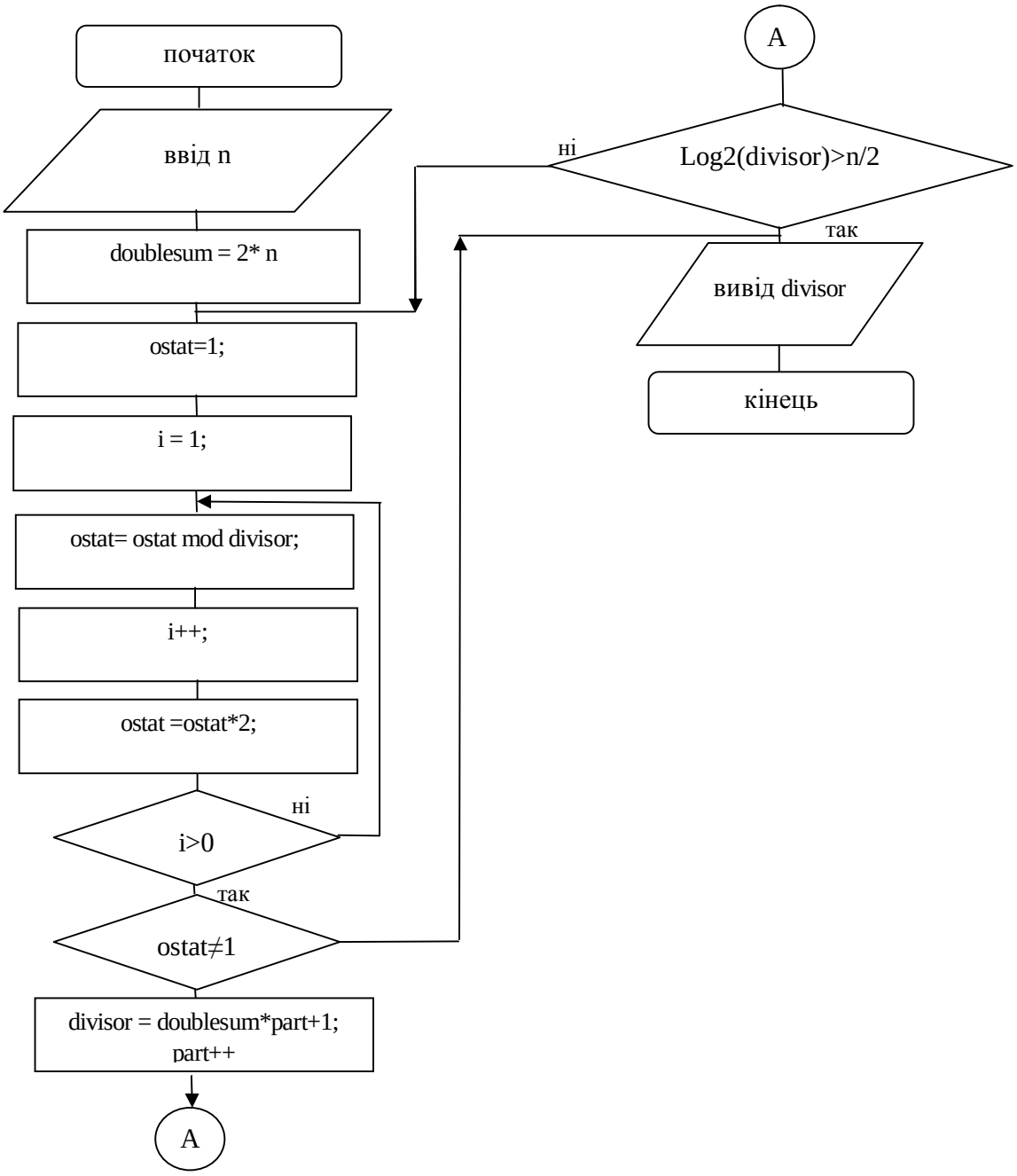

Рис. 3. Блок-схема алгоритму факторизації ВРЧ Мерсена прямим перебором

Складність алгоритму полягає у складності знаходження залишків і надлишкової перевірки чисел, які заздалегідь не є простими числами і не можуть бути дільниками числа Мерсена.

Загальновідома форма числа Мерсена $2^n - 1$[4]. Для процесу факторизації використовуватимемо значення n. Дільник числа Мерсена має форму *2nk+1* [4].

Особливістю розробленого алгоритму є використання властивостей співмножників *2n* і *k* щодо простих модулів. Це дає змогу на декілька порядків збільшити швидкодію.

Обчислювальна складність запропонованого алгоритму значно зменшується, її можна оцінити як $\Theta(N^{1/2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11} \cdot \frac{12}{13})$. Це означає, що залишки *k* за простими модулями дозволяють виключити понад 1/3 діапазону перебору всіх можливих дільників. На рис. 4 подано блок-схему запропонованого алгоритму факторизації ВРЧ Мерсена.

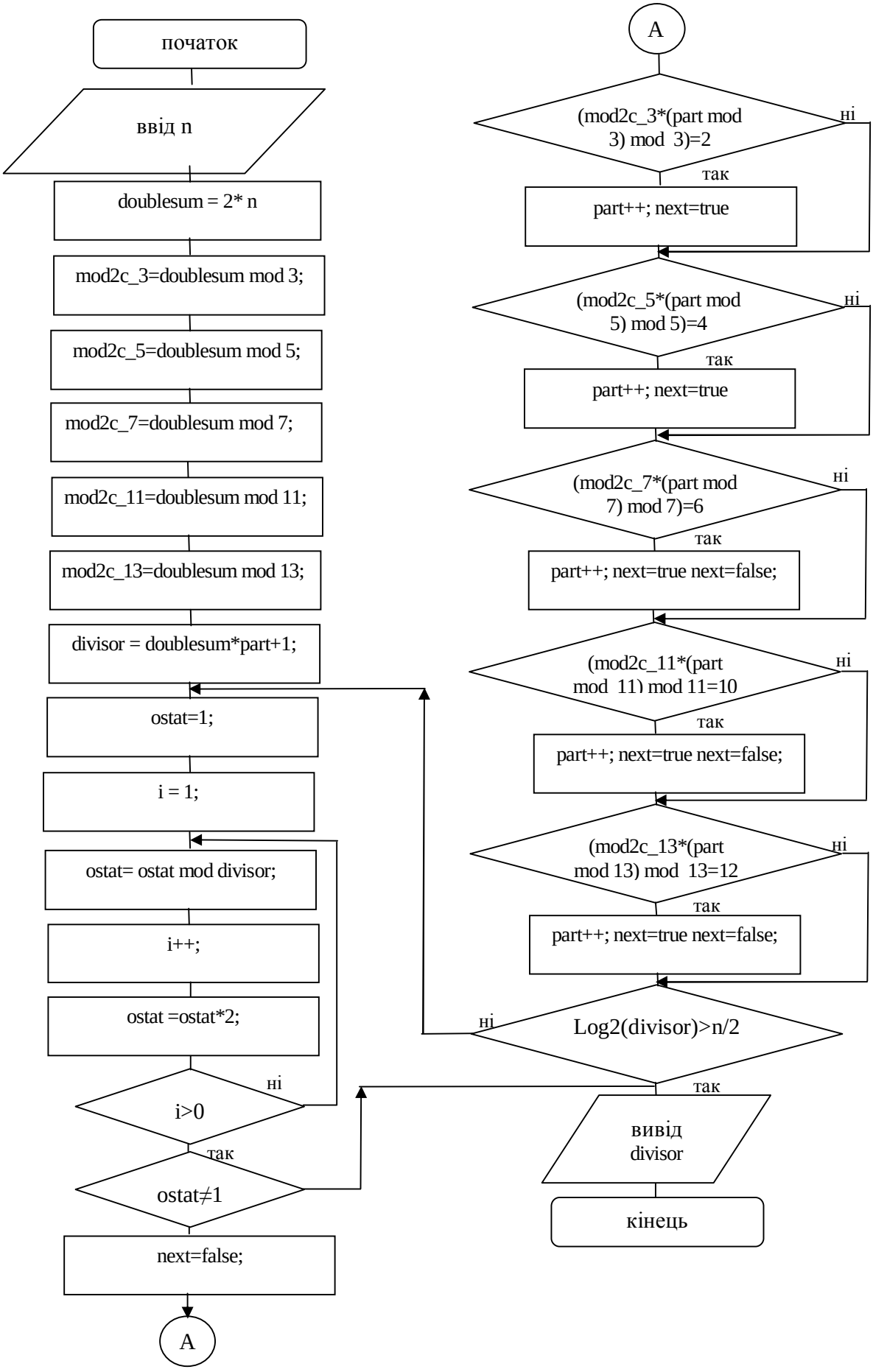

Рис. 4. Блок-схема алгоритму факторизації ВРЧ Мерсена

Оскільки найменшим дільником ВРЧ Мерсена повинно бути просте число, то, як показано на рис. 4, для факторизації ВРЧ Мерсена використовується перевірка залишків множника *k* (на рис. 4 він позначений *part*). Ця операція виконується, щоб уникнути надлишкових перевірок непростих дільників. Кількість простих модулів, за якими виконується перевірка, можна збільшувати до певного числа, поки ефективність алгоритму почне падати.

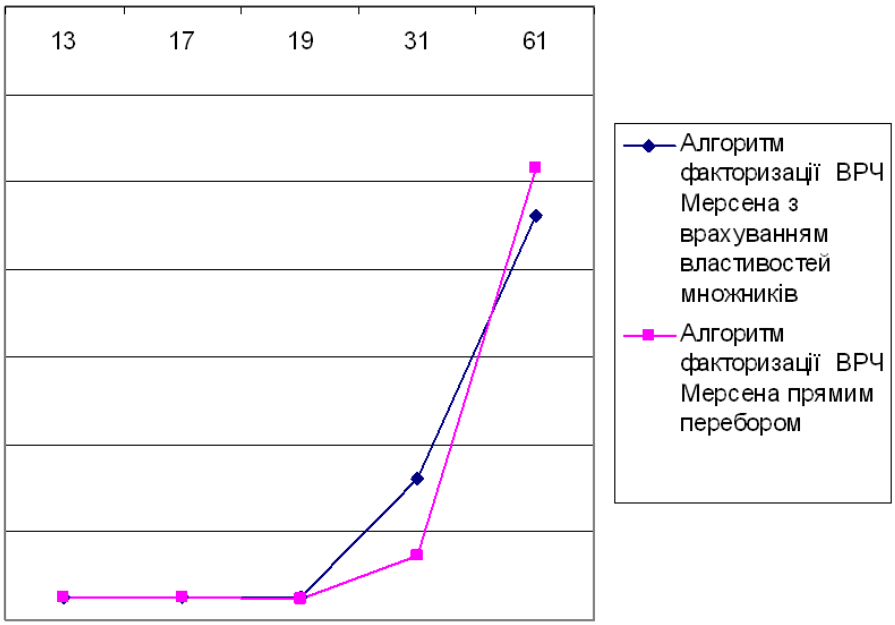

Рис. 5. Порівняння часових характеристик роботи алгоритмів на логарифмічній шкалі

На рис. 5 наведено схематичні графіки порівняння часових характеристик алгоритмів на логарифмічній шкалі, які свідчать про великі переваги алгоритму факторизації ВРЧ Мерсена з урахуванням властивостей множників над алгоритмом факторизації ВРЧ Мерсена прямим перебором, які зростатимуть експоненційно.

Висновки

Аналіз наявних методів та алгоритмів опрацювання великорозрядних чисел показує перспективність їх розвитку, оскільки вимоги до розрядності простих чисел лінійно зростають.

Цей алгоритм вимагає менше обчислювальних ресурсів – порівняно з наявними на 1–2 порядки, крім того, він придатний для знаходження множника числа Мерсена.

Розроблений метод можна розпаралелити і його реалізація за допомогою кластера дасть змогу наблизитись до пошуку та факторизації наступних ВРЧ Мерсена.

1. Задірака В.К., Олексюк О.С. Комп'ютерна арифметика багаторозрядних чисел: наукове видання. – К.: 2003. – 264 с. 2. Ленг Т. Алгебраические числа. – М.: Мир, 1966. – 225 с. 3. Николайчук Я.М. Теорія джерел інформації. – Тернопіль: ТзОВ „Терно–граф", 2010. – 536 с. 4. www.mersenne.org Інтернет-проект "Пошук великих чисел Мерсена". 5. Хетагуров А.Я., Руднев Ю.П. Повышение надежности цифровых устройств методами избыточного кодирования. – М.: Энергия, 1974. – 272 с. 6. Івасьєв С.В, Метод знаходження залишків великорозрядних чисел в базисі Радемахера // Поступ в науку: Зб. наук. праць Бучацького інституту менеджменту і аудиту. – Бучач. – 2011. – №7. Т1. – С. 88–91.