УДК 681.32

М.Л. Глинська[1], Д.В. Лісковецький[2], С.В. Івасьєв[2]

[1]Галицький коледж ім. В. Чорновола

[2]Тернопільський національний економічний університет

АЛГОРИТМ КОДУВАННЯ ПРОСТИХ БАГАТОРОЗРЯДНИХ ЧИСЕЛ

Вступ. При реалізації алгоритмів опрацювання багаторозрядних простих чисел в задачах вибору системи взаємно простих модулів для процесорів теоретико-числових базисів (ТЧБ) Крестенсона, пошуку найбільшого спільного дільника, виявлення квадратичного лишку, виконання арифметичних операцій модульної арифметики виникає необхідність зберігання та генерування великих масивів багаторозрядних простих чисел. Генерування та зберігання багаторозрядних простих чисел, представлених повнорозрядними двійковими кодами, є неефективним у зв'язку з тим, що потребує великих об'ємів пам'яті.

1. Дослідження розподілу простих чисел.

Теорема про розподіл простих чисел стверджує, що кількість $\pi(n)$ простих чисел на відрізку від 1 до n зростає із зростанням n, як $\frac{n}{\ln n}$, тобто $\frac{\pi(n)}{n/\ln n} \to 1,\ n \to \infty$. Оцінка об'ємів пам'яті згідно наведеної теореми приведена в таблиці 1.

Таблиця 1 – Верхня оцінка розподілу простих чисел

Розрядність	Кількість	Об'єм пам'яті
2^8	64	64 байти
2^{10}	256	2 КБ
2^{16}	16384	32 КБ
2^{32}	1073741824	4 Гб
2^{64}	4611686018427387904	36 Гб
2^{128}	8,5070591730234615865843651857942e+37	2^{213} Терабайт
2^{256}	2,894802230932904885589274625217 2e+76	2^{426} Йотабайт
2^{512}	3,351951982485649274893506249551 5e+153	*
2^{1024}	4,494232837155789769323262976972 6e+307	*

Зростання верхньої оцінки об'єму пам'яті для повнорозрядного зберігання простих двійкових чисел показано на рисунку 1.

Побудований графік із змінною шкалою, в якому відображені верхні оцінки необхідного об'єму для збереження простих чисел.

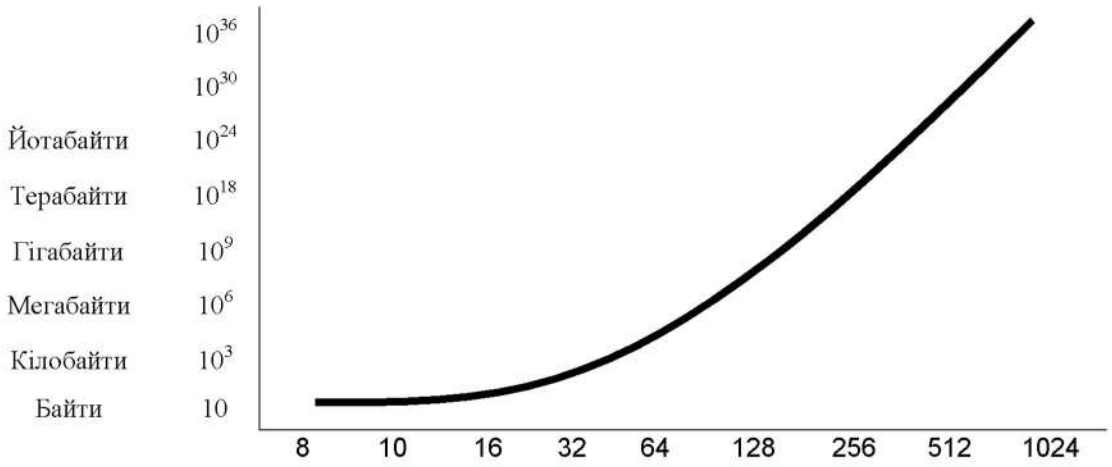

Рисунок 1 - Оцінка об'єму пам'яті для повнорозрядного зберігання простих двійкових чисел

З графіка видно, що об'єм пам'яті, необхідний для зберігання n-розрядних простих чисел до 32 розрядів, становить 4 Гб , для 64 розрядів - 36 Гб, а при 128 - 2^{213} Терабайт, оскільки при опрацюванні окремих задач теорії чисел розрядність простих чисел може сягати 512 біт, що відповідає надзвичайно великим об'ємам необхідної пам'яті, тому актуальною є наукова задача більш компактного зберігання великих масивів багаторозрядних простих чисел.

Можливість більш компактного зберігання простих багато розрядних чисел (БРЧ) може бути реалізована за рахунок надлишковості багаторозрядних двійкових кодів, оскільки різниця між двома простими БРЧ може не перевищувати 10-20 біт. Причому інформативна частина простого числа знаходиться в 20-30 бітах молодших розрядів при ідентичності сотень старших бітів, починаючи з 32 -64 біт. Для прикладу візьмемо числа з інтервалу $2^{20} \div 2^{64}$:

1052629_{10} =10000000111111010101 (2^{20});

2147487701_{10}=10000000000000000000111111010101 (2^{32});

9223372036854779861_{10}=10000000000000000000000000000000000000000000000000000000111111010101(2^{64});

При цьому в двійкових кодах багаторозрядних простих чисел (БРПЧ)

при активній зміні бітів молодших розрядів в старших розрядах велике число одиниць або нулів може обчислюватись тисячами, що є основою методу компактного кодування БРПЧ. В роботах [1, 2] запропонований метод компактного кодування БРПЧ, суть якого полягає в тому, що в пристроях пам'яті запам'ятовується певне число молодших розрядів, а 1 біт використовується для ідентифікації наскрізних переносів у старші розряди, а коди старших розрядів визначаться шляхом підрахунку числа переносів, які ідентифіковані бітом синхронізації, розподіл якого в середньому до 20 простих чисел. Тобто у діапазоні до 2^{1024} буде знаходитись 2^{51} бітів синхронізації.

Таблиця 2 – Послідовність простих чисел з однаковим закінченням

4194389 100000000000 0000101 0101	4195493 100000000000 1001010 0101
4194581 100000000000 0010001 0101	4195573 100000000000 1001111 0101
4194661 100000000000 0010110 0101	4195589 100000000000 1010000 0101
4194677 100000000000 0010111 0101	4195621 100000000000 1010010 0101
4194917 100000000000 0100110 0101	4195861 100000000000 1100001 0101
4195157 100000000000 0110101 0101	4195973 100000000000 1101000 0101
4195189 100000000000 0110111 0101	4196149 100000000000 1110011 0101
4195253 100000000000 0111011 0101	4196341 100000000000 1111111 0101

Висновки.

Таким чином, для зберігання об'єму простих чисел розрядністю до 1024 за попередніми оцінками потрібно 1048576 байт. Для збереження цілого числа в двійковій системі використовуються всі байти, які несуть значення числа. В результаті проведених досліджень та аналізу переліку простих чисел отримано результати, які свідчать про те, що числа з однаковими молодшими бітами можна представити у вигляді трьох частин. Їх розміри залежать від розрядності простого числа та кількості бітів в обраному закінченні (таблиця 2).

Перелік джерел.

1. Івасьєв С.В. Метод зберігання простих великорозрядних чисел у базисі Радемахера / С.В. Івасьєв, М.М. Касянчук, І.З. Якименко // Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)" Київ: Інститут кібернетики імені В.М. Глушкова НАН України, 2013. – С. 142-144.

2. Gbolagade K.A. Residue Number System Operands to Decimal Conversion for 3-Moduli Sets, / K.A.Gbolagade, S. D. Cotofana // Proceedings of 51st IEEE Midwest Symposium on Circuits and Systems (MWSCAS-08). - Knoxville, USA.,2008. - P. 791-794.

3. Івасьєв С.В. Метод організації компактної бібліотеки простих чисел великої розрядності / С.В. Івасьєв //Збірник матеріалів міжнародної наукової координаційної наради «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління» (ICSM) – Тернопіль, 2014. – С. 86-89.