МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОБЧИСЛЮВАЛЬНІ МЕТОДИ

doi:https://doi.org/10.15407/emodel.40.05.003

УДК 511:003.26.09

С.Д. Винничук, д-р техн. наук, **В.М. Міська**, аспірант
Інститут проблем моделювання в енергетиці ім. Г.Е. Пухова НАН України
(Україна, 03164, Київ, вул. Генерала Наумова, 15,
тел. +380734095726; e-mail: vynnychuk@i.ua; vitalii.misko@gmail.com)

Метод множинного квадратичного *k*-решета цілочисельної факторизації

Запропоновано модифікацію методу квадратичного решета (QS), в якій для пошуку *B*-гладких чисел використовуються поліноми $X^2 - kN$. На відміну від методів QS та множинного поліноміального квадратичного решета (MPQS) в запропонованому методі множинного квадратичного *k*-решета (MQ*k*S) використовується загальна факторна база (ФБ), яка деталізується при кожному значенні *k*. В алгоритмі враховано, що кількість *B*-гладких є відносно більшою при менших значеннях чисел з інтервалу просіювання. Цей факт підтверджено даними чисельних експериментів. Описано кроки алгоритму та ідеї їх реалізації. На основі чисельних експериментів показано, що за допомогою методу MQ*k*S можна зменшити в середньому час формування множини *B*-гладких порівняно з методом QS при зменшенні розміру ФБ.

Ключові слова: цілочисельна факторизація, метод квадратичного решета, множинне решето.

Постановка задачі. На даний часъ криптоалгоритм RSA реалізовано у багатьох комерційних системах. Він використовується у web-серверах і браузерах для захисту трафіку, у електронній пошті для забезпечення конфіденційності та автентичності і є ключовою технологією у системах електронних платежів. Найбільш поширена атака на цей криптоалгоритм основана на факторизації публічного ключа *N*, що є добутком двох простих чисел [1—3]. Якщо факторизація успішна, усі повідомлення, зашифровані відкритим ключем, можуть бути прочитані.

Серед багатьох методів факторизації метод квадратичного решета (QS) посідає друге місце у списку найшвидших алгоритмів, поступаючись тільки методу решета числового поля, а для чисел розміром до 110 десяткових знаків і досі є найкращим [4]. Основна ідея методу QS полягає у пошуку *B*-гладких чисел, тобто у яких різниця

$$y = X^2 - N, \tag{1}$$

де $X^2 = x_0 + x, x_0 = [\sqrt{N}] + 1$, розкладається у добуток простих чисел — елементів факторної бази (ФБ).

У науковій літературі описано два підходи до визначення елементів ФБ. Згідно [4] для цього визначається границя гладкості B — число, що обмежує зверху величину простих чисел — елементів бази. Самі ж елементи бази визначаються на основі обчислення значення символу Лежандра. Проте при обмеженнях на границю гладкості трапляються випадки, коли неможливо отримати достатню кількість B-гладких чисел. Тоді збільшують границю гладкості та число елементів ФБ і пошук B-гладких повторюється.

У роботі [5] запропоновано не обмежуватися границею гладкості, а визначати кількість елементів ФБ за формулою

$$L^a = (e^{\sqrt{\ln N \ln\ln N}})^{\sqrt{2}/4}. \quad (2)$$

Для факторизації N потрібно знайти $L^a + 2$ B-гладких чисел. Для їх визначення необхідно знаходити остачі в (1) та перевіряти можливість розкладання на прості множники елементів ФБ для великої кількості x. Кількість пробних значень x пропонується вибирати з інтервалу просіювання $[-L^b, L^b]$, де радіус просіювання L^b визначається за формулою [5]

$$L^b = (e^{\sqrt{\ln N \ln\ln N}})^{3\sqrt{2}/4} = (L^a)^3. \quad (3)$$

Факторизація чисел порядку 10^{129} та більших потребує значних обчислювальних ресурсів (для числа N, відомого як RSA-129, було задіяно мережу з 1600 комп'ютерів, що працювала 220 днів, було сформовано матрицю лінійних рівнянь з 524338 невідомими, яку суперкомп'ютер розв'язував протягом двох днів [6]). Тому розробка способів зниження обчислювальної складності алгоритму методу QS є надзвичайно актуальною.

Задачі дослідження. Основні ідеї підходів, що можуть забезпечувати зниження обчислювальної складності алгоритму методу QS, пов'язані зі зменшенням області просіювання та розміру ФБ. Наприклад у роботах [7—9] зазначено, що спроба зменшення числа елементів ФБ призводить до збільшення інтервалу просіювання і може спричинити зростання обчислювальної складності. При цьому необхідно отримувати більшу кількість B-гладких та розв'язувати систему рівнянь більш високого порядку, що також може впливати на зростання обчислювальної складності.

Для алгоритму квадратичного решета було запропоновано ряд модифікацій, які пов'язані з прискоренням процесу просіювання та вирішенням матриці. Для збільшення числа можливих B-гладких чисел без збільшення інтервалу просіювання пропонується запам'ятовувати функції $y(x) = y_1(x)\, y_2(x)$ такі, в яких $y_1(x)$ — B-гладке число, а $B < y_2(x) < B^2$ [10]. За

наявності двох таких чисел y з однаковим значенням y_2 їх добуток стане B-гладким. Існує також варіант, коли $y_2(x)$ є добутком двох простих чисел, які перевищують границю гладкості B та виконується умова $B^2 < y_2(x) < B^3$. Такі способи отримання додаткової кількості B-гладких чисел використано при розкладанні на множники числа RSA-129. Як зазначено в [11, 12], подальший розвиток ідеї великих множників (трьох і більше) викликає додаткові ускладнення і вважається неефективним.

У роботі [13] запропоновано перевіряти, чи не виявиться $y_2(x)$ квадратом цілого числа. Для таких чисел немає потреби шукати пару, як у попередньому варіанті модифікації, їх називають умовно B-гладкими і причисляють до множини B-гладких. Проблемним є питання, коли перевіряти, чи буде $y_2(x)$ точним квадратом. Перевірка кожного значення функції $y_2(x)$ потребує значного числа операцій ділення та обчислення кореня. Тому при такому способі отримання додаткових B-гладких чисел спостерігається значне зростання обчислювальної складності, що неприйнятно при факторизації великих чисел. Умови, при яких цей підхід може бути ефективним, потребують окремих досліджень.

У всіх зазначених роботах вважалося, що на етапі вирішення матриці обов'язкова наявність кількості B-гладких чисел, не меншої за $L^a + 2$. У роботі [14] запропоновано модифікацію алгоритму QS, в якій на основі поточного аналізу B-гладких чисел для кожного i-го B-гладкого числа визначається найбільший порядковий номер елемента ФБ $p(i)$, для якого непарним буде показник степеня в розкладанні B-гладкого. Якщо в ході отримання множини B-гладких виявиться, що знайдено $L_{\max} + 2$ B-гладких чисел, для яких $p(i) \le L_{\max}$ і $L_{\max} < L^a$, то можна зменшити область просіювання і розмір матриці. При цьому число додаткових (стосовно базового алгоритму QS) елементарних операцій з малими числами не перевищує 0,5 $(L^a)^2$.

В модифікованому алгоритмі, наведеному у [15], досягти зменшення області просіювання та розміру матриці можна у випадку, коли у множині $L_{\max} + 2$ B-гладких чисел всі непарні показники степенів множників зачисляють до порядкових номерів елементів ФБ, які не перевищують $L_{\max} \le L^a$. Проте існують випадки, коли розв'язок задачі факторизації можливий при значно меншому числі B-гладких, коли елементи ФБ, які в них використовуються, можуть розміщуватися довільно, а не тільки серед найменших їх значень. У [15] такий варіант модифікації методу QS реалізується паралельно з процесами просіювання зі знаходженням B-гладких чисел та нульового вектора при діагоналізації матриці векторів степенів. Запропоновані в роботах [13—15] способи зменшення обчислювальної складності на основі використання умовно B-гладких чисел, достатнього числа

B-гладких та діагоналізації матриці на ходу дозволили більше ніж вдвічі зменшити обчислювальну складність тільки для деяких чисел *N*, але в загальному випадку обчислювальна складність для чисел, що перевищують 10^{110}, зменшується в межах 4—6%, що не можна вважати суттєвим.

Серед модифікацій алгоритму QS окремо слід виділити ідею методу множинного поліноміального квадратичного решета (MPQS) [16, 17]. В запропонованому методі крім полінома (1) розглянуто ряд інших поліномів виду

$$z_{a,b}(x) = (ax+b)^2 - N = a^2x^2 + 2abx + b^2 - N, \qquad (4)$$

де *a*, *b* — спеціально підібрані цілі числа; *x* вибирається з інтервалу просіювання [–*L*, *L*]. Існує зв'язок між величиною інтервалу просіювання, що визначається числом *L*, та кількістю поліномів $z_{a,b}(x)$. При малих значеннях *L* необхідно генерувати багато поліномів $z_{a,b}(x)$, для яких слід визначати параметри *a*, *b* та формувати ФБ, що є затратною процедурою. При великих значеннях *L* число поліномів буде меншим, але при просіюванні необхідно обробляти досить великі значення залишків: $q(x) = z_{a,b}(x)/a = ax^2 + 2bx + c$, де $c = (b^2 - N)/a$.

При аналізі оцінки обчислювальної складності методу QS [8] використовується середнє значення пробних *x* з інтервалу просіювання для отримання одного *B*-гладкого числа. Проте, як показують чисельні експерименти, *B*-гладкі числа розміщуються на інтервалі просіювання в середньому за деяким законом, загальною характеристикою якого є те, що зі збільшенням модуля *x* зростає кількість *x*, які слід просіяти. Використання такої обставини при вирішенні задачі факторизації в літературних джерелах не виявлено.

Принциповим моментом для методів QS і MPQS є також використання поліномів (1) та (4), у яких входить значення (– *N*). В той же час, при пошуку пари чисел *A* і *B* для досягнення рівності

$$A^2 = B^2 (\mathrm{mod}\, N), \qquad (5)$$

можна використати множину поліномів

$$y = x^2 - kN, \qquad (6)$$

де *k* — натуральне число, а побудова нових поліномів є дуже простою. Покажемо це на прикладі.

Нехай $N = 86327$, $L^a = 6$ згідно (2). Візьмемо радіус просіювання $L^b = 2L^a = 12$ та $k = 1 \div 2L^a$. Елементами ФБ вибираємо перші L^a найменші прості

числа. Перебираючи всі варіанти значень k та x, отримаємо B-гладкі числа, представлені в табл. 1, де для значень k, які містять дільники, що є квадратами простого числа t, значення $x_0 + x$ не діляться на t: $x_0 = [\sqrt{kN}]+1$.

Аналіз даних табл. 1 показує, що рівність (5) можна отримати на основі добутку B-гладких, що відповідають x, які дорівнюють 777 і 1007. Рішення отримаємо при x = 509. В обох випадках це дозволяє знайти множники N чисел 173 та 499. Але при отриманні рівності (5) на основі добутку значень x, рівних 657, 659 та 664, корінь буде хибним.

Наведений приклад свідчить про можливість отримати корінь, використовуючи співвідношення (6). В результаті було отримано 12 B-гладких чисел при $x = 25 \cdot 12 = 300$. При використанні базового методу QS ФБ з шести елементів міститиме прості числа 2, 17, 23, 29, 53 і 61, а для просіяних x від 30 до 558 (всього 529 пробних x) буде отримано всього п'ять B-гладких замість необхідних восьми. Можна очікувати, що метод, який ґрунтується на рівності (6), зможе забезпечити зменшення обчислювальної складності процесу просіювання та загального часу розв'язування задачі факторизації.

Таблиця 1. **B-гладкі числа для N = 86 327**

k	x_0	x	$x_0 + x$	B-гладке	Показник степеня елемента ФБ						
					–1	2	3	5	7	11	13
1	294	Відсутні									
2	416	–1	415	–429	1	0	1	0	0	1	1
		12	428	10530	0	1	4	1	0	0	1
3	509	0	509	100	2	0	2	0	0	0	0
4	588	Відсутні									
5	657	0	657	14	0	1	0	0	1	0	0
		2	659	2646	0	1	3	0	2	0	0
		7	664	9261	0	0	3	0	3	0	0
6	720	–1	719	–1001	1	0	0	0	1	1	1
7	778	–1	777	–560	1	4	0	1	1	0	0
		5	783	8800	0	5	0	2	0	1	0
		–1	767	–16000	1	7	0	3	0	0	0
8	832	–1	831	–55	1	0	0	1	0	1	0
9	882	Відсутні									
10	930	"									
11	975	"									
12	1018	–11	1007	–21875	1	0	0	5	1	0	0

Метод факторизації, в якому пропонується використовувати поліноми (6), назвемо множинним квадратичним *k*-решетом (Multiple Quadratic *k*-Sieve (MQ*k*S)). Будемо досліджувати алгоритм факторизації MQ*k*S, оцінюючи його обчислювальну складність у порівнянні з методом QS.

Розміщення *B*-гладких в діапазоні інтервалу просіювання. Інтуїтивно зрозуміло, що чим меншою буде остача в (1), (4) чи (6), тим більшою повинна бути ймовірність розкладання її на прості множники — елементи ФБ. Тому перше завдання, яке вирішувалося при розробці методу MQ*k*S, полягало в отриманні оцінок стосовно розміщення *B*-гладких в діапазоні інтервалу просіювання. При проведенні чисельних експериментів з'ясувалося, що для кожного конкретного *N* при однакових значеннях кількості елементів ФБ та розміру області просіювання різною була кількість *B*-гладких чисел і розподіл відповідних їм *x* в області просіювання. Тому для отримання оцінок, які можна було б використати в подальшому, було прийнято наступні правила проведення чисельних експериментів.

1. Множина *N*, що використовується при отриманні середніх оцінок розміщення *B*-гладких в діапазоні інтервалу просіювання, формується як добуток двох різних простих чисел, *p* і *q* ($p < q$), де *p* і *q* вибиралися з множини простих чисел, з порядковими номерами, що слідують підряд.

2. Для кожного *N* зі сформованої множини встановлюються єдині значення розміру ФБ L^a згідно (2) і для кожного *N* визначається радіус просіювання L^b за формулою (3).

3. Для оцінки розміщення *B*-гладких в діапазоні інтервалу просіювання використовуються дані тільки для тих *N*, для яких отримано L^a *B*-гладких остач (1).

Першу серію чисельних експериментів було проведено для $m = 14$ множин чисел $N = pq$, кожна з яких містила 500000 варіантів. В кожній множині *m* множники *p* — це прості числа з порядковими номерами від 1001 до 2000, де номер 1 — це число 2; 2 — число 3; 3 — число 5 і т.д. Для *m*-ї множини прості числа *q* вибиралися як порядкові номери простих чисел від $2001 + 500\,m$ до $2500 + 500\,m$. Для кожної з таких множин розглядалися варіанти числа *fb* елементів ФБ, яке дорівнювало 8, 16, 24, 32, 48 та 64, де 16 відповідає L^a, що визначалося за формулою (2) для середнього значення *N* серед аналізованих множин: 8 — $0{,}5L^a$; 16 — L^a;24 — $1{,}5L^a$; 32 — $2L^a$; 48 — $3L^a$ та 64 — $4L^a$.

Для визначення середнього значення кількості *x*, необхідних для отримання кожного *j*-го *B*-гладкого числа ($k = 1 \div fb$) було розраховано сумарну величину sum(*j*) значень *x* для всіх *sc* значень *N*, що відповідають правилу 3, після чого отримане сумарне значення ділилося на *sc*. Тобто се-

реднє значення $xx\,(j)$ розраховано за формулою $xx\,(j)=\mathrm{sum}\,(j)/sc$. Для оцінки залежності, що відповідає варіанту множини та розміру ФБ, формувалися перші ($dx\,(j)=xx\,(j+1)-xx\,(j)$), другі ($d2x\,(j)=dx\,(j+1)-dx\,(j)$) та треті ($d3x\,(j)=d2x\,(j+1)-d2x\,(j)$) різниці середніх значень. Фактичні дані для $m=1$, $m=7$ та $m=14$ при $fb=8$ наведено в табл. 2 з використанням чотирьох десяткових цифр. Аналогічні дані при $m=1$ і $fb=16$, 32 та 64 для перших 16 B-гладких надано у табл. 3.

Дані, наведені в табл. 2 і 3, є підтвердженням наступних висновків, отриманих за результатами чисельних експериментів.

1. Для всіх варіантів чисел N та кількості елементів ФБ спостерігається зростання змінних xx та dx.

2. Для числа елементів ФБ $fb = L^a$ функція $xx\,(j)$ практично є параболою, оскільки треті різниці $d3x$ постійно змінюють знак.

3. Для числа елементів ФБ $fb < L^a$ функція $xx\,(j)$ зростає швидше ніж парабола, оскільки треті різниці $d3x$ додатні, їх значення спочатку зменшуються, а потім стабілізуються на додатному значенні.

4. Для числа елементів ФБ $fb > L^a$ функція $xx\,(j)$ зростає як парабола, проте додатні значення других різниць $d2x$ спочатку зменшуються, а потім стабілізуються на додатному значенні.

5. Із зростанням значення N зростають середні значення $xx\,(j)$ для всіх j.

6. Зі збільшенням числа елементів ФБ зменшуються середні значення $xx\,(j)$ для всіх j.

Таблиця 2. **Розподіл середніх значень *B*-гладких чисел у діапазоні інтервалу просіювання для *fb* = 8**

j	*m* = 1				*m* = 7				*m* = 14			
	xx	*dx*	*d*2*x*	*d*3*x*	*xx*	*dx*	*d*2*x*	*d*3*x*	*xx*	*dx*	*d*2*x*	*d*3*x*
0	0	21,35	39,01	14,87	0	26,69	50,22	19,83	0	30,53	58,71	24,52
1	21,35	60,36	53,88	10,53	26,69	76,91	70,05	16,71	30,53	89,24	83,24	20,89
2	81,71	114,2	64,42	9,581	103,6	147	86,75	17,41	119,8	172,5	104,1	20,26
3	196	178,7	73,99	13,7	250,5	233,7	104,2	15,69	292,3	276,6	124,4	22,45
4	374,6	252,6	87,69	8,859	484,3	337,9	119,8	14,88	568,9	401	146,8	12,01
5	627,2	340,3	96,55	8,321	822,1	457,7	134,7	10,68	969,9	547,8	158,9	14,6
6	967,6	436,9	104,9		1280	592,4	145,4		1517	706,7	173,5	
7	1404	541,8			1872	737,7			2224	880,2		
8	1946				2610				3104			
sc	295368 (59,07%)				240086 (48,02%)				208923 (41,78%)			

7. Для поліноміальної функції *xx* (*j*) значення коефіцієнта при j^1 не перевищує значення коефіцієнта при j^2.

На основі отриманої інформації та наведених висновків можна припустити, що при пошуку *B*-гладких з використанням багатьох поліномів з малим радіусом просіювання, є ймовірність отримати модифікацію алгоритму методу QS (MPQS), обчислювальна складність якого буде нижчою, ніж QS. Цього можна очікувати, оскільки *B*-гладких чисел більше при малих значеннях *x* з інтервалу просіювання.

Середнє значення числа елементів ФБ при фіксованій границі гладкості для поліномів (6). Одна з основних проблем, пов'язаних з використанням різних функцій (6) для формування множини *B*-гладких чисел, полягає у тому, що для кожної з них необхідно формувати свою ФБ. В методі MQ*k*S пропонується використовувати загальну ФБ (ЗФБ) для всіх значень *k*, яка містить прості числа до границі гладкості *B*.

Таблиця 3. **Розподіл середніх значень *B*–гладких чисел у діапазоні інтервалу просіювання для перших 16 *B*-гладких**

j	*fb* = 16				*fb* = 32				*fb* = 64			
	xx	*dx*	*d2x*	*d3x*	*xx*	*dx*	*d2x*	*d3x*	*xx*	*dx*	*d2x*	*d3x*
0	0	6,463	5,315	0,541	0	2,848	1,079	–0,1	0	1,897	0,382	–0,078
1	6,463	11,78	5,856	–0,135	2,848	3,927	0,98	–0,122	1,897	2,279	0,304	0,039
2	18,24	17,63	5,721	–0,164	6,775	4,907	0,858	–0,122	4,177	2,583	0,342	–0,098
3	35,87	23,36	5,558	–0,262	11,68	5,765	0,736	–0,084	6,759	2,925	0,244	–0,005
4	59,23	28,91	5,296	–0,07	17,45	6,501	0,652	–0,037	9,684	3,169	0,24	–0,032
5	88,14	34,21	5,226	–0,078	23,95	7,153	0,615	–0,014	12,85	3,409	0,207	–0,009
6	122,4	39,43	5,148	0,107	31,1	7,768	0,601	–0,019	16,26	3,616	0,199	–0,002
7	161,8	44,58	5,255	–0,265	38,87	8,369	0,582	–0,004	19,88	3,815	0,197	–0,045
8	206,4	49,84	4,989	0,134	47,24	8,95	0,578	–0,048	23,69	4,012	0,15	0,003
9	256,2	54,83	5,123	0,28	56,19	9,529	0,53	0,032	27,71	4,161	0,153	–0,009
10	311	59,95	5,403	0,057	65,72	10,06	0,561	–0,064	31,87	4,315	0,144	–0,001
11	371	65,35	5,461	–0,213	75,78	10,62	0,497	–0,003	36,18	4,459	0,143	–0,023
12	436,3	70,81	5,247	0,638	86,4	11,12	0,494	0,025	40,64	4,602	0,12	0,026
13	507,1	76,06	5,886	–0,513	97,51	11,61	0,52	–0,042	45,24	4,721	0,146	–0,048
14	583,2	81,95	5,372		109,1	12,13	0,478	0,002	49,96	4,867	0,097	0,028
15	665,2	87,323			121, 3	12,61	0,48	–0,013	54,83	4,964	0,125	–0,016
16	752,3				133,9	13,09	0,467	0,03	59,8	5,09	0,109	–0,014
sc	495 238 (99,0476%)				499 966 (99,9932%)				500 000 (100%)			

За результатами чисельних експериментів згідно висновку 6, для однієї і тієї ж області просіювання число отримуваних B-гладких чисел залежить від кількості елементів ФБ. Тому важливою є оцінка середнього числа елементів ФБ для різних значень N та множини k при фіксованій границі гладкості. Для отримання такої інформації було проведено другу серію чисельних експериментів. Як і для першої серії, формувалися множини чисел N. Було сформовано 28 множин, кожна з яких містила 100000 варіантів.

Для множин $m = 1 \div 7$ множники p — це прості числа з порядковими номерами від 501 до 600, а для m-ї множини прості q обиралися як порядкові номери простих чисел в діапазоні від $1501 + 1000\,m$ до $2500 + 1000\,m$. Для множин $m = 8 \div 14$ множники p — це прості числа з порядковими номерами від 1001 до 1100, а для m-ї множини прості q обиралися як порядкові номери простих чисел від $1501 + 1000\,(m - 7)$ до $2500 + 1000\,(m - 7)$. Для множин $m = 15 \div 21$ множники p — це прості числа з порядковими номерами від 1501 до 1600, а для m-ї множини прості q — це порядкові номери простих чисел від $1501 + 1000\,(m - 14)$ до $2500 + 1000\,(m - 14)$. Для множин $m = 22 \div 28$ множники p — це прості числа з порядковими номерами від 2001 до 2100, а для m-ї множини прості q — це порядкові номери простих чисел від $1501 + 1000\,(m - 21)$ до $2500 + 1000\,(m - 21)$.

Для кожної з таких множин було розглянуто варіанти границі гладкості, яка визначалася порядковим номером простого числа L^a та $2L^a$. При цьому K — максимальні значення для k у співвідношеннях (6) — дорівнювали $2L^a$, $4L^a$ та $(L^a)^2$, але не розглядалися k, які діляться націло на квадрат простого числа, що не перевищує $\sqrt{B}$. Для множин $m = 22 \div 28$ додатково розглядалися варіанти границі гладкості $B = 4L^a$. Загальне число варіантів розрахунків склало $28 \cdot 3 \cdot 2 + 7 \cdot 3 = 189$. За результатами розрахунків встановлено, що середнє число елементів ФБ для всіх варіантів розрахунків перевищує половину кількості простих чисел ЗФБ. При цьому найменше значення становило 50,1572% (при $m = 2$, $B = L^a$, $K = 2L^a$), а найбільше — 54,3208% (при $m = 5$, $B = L^a$, $K = (L^a)^2$).

За отриманими результатами можна попередньо оцінити затрати на формування множини B-гладких чисел. Нехай границя гладкості B визначена за умови, що число простих, які не перевищують B, дорівнює $2L^a$. Радіус інтервалу просіювання становить $2L^a$, а $k = 1 \div 2L^a + 2$. Визначимо ймовірне середнє число B-гладких чисел, яке можна при цьому отримати. Оскільки середнє число елементів ФБ перевищує половину кількості простих чисел, не більших за границю гладкості B, можна припустити, що для кожного k розмір ФБ буде $fb \geq L^a$. Але тоді B-гладкі в діапазоні інтервалу просіювання розміщуються за квадратичним законом, де нульовому

B-гладкому відповідає 0, а *B*-гладкому з номером L^a — деяке значення з інтервалу просіювання. Інтервал просіювання містить $2L^b + 1$ пробне значення *x*, де $L^b = (L^a)^3$. Тому в гіршому випадку порядковий номер *x* з інтервалу просіювання може дорівнювати $2 (L^a)^3 + 1$.

На основі квадратичного закону розміщення *B*-гладких, де для полінома другого степеня *xx* (*j*) значення коефіцієнта при j^1 не перевищує значення коефіцієнта при j^2, обчислимо необхідну кількість пробних *x*, щоб знайти перше *B*-гладке. Нехай коефіцієнти при j^1 та j^2 для полінома співпадають і дорівнюють *c*. Тоді $xx(j) = cj^2 + cj$. Коефіцієнт *c* визначимо за умови, що $xx(j) = 2(L^a)^3 + 1$ при $j = L^a$. Тоді отримаємо

$$c = \frac{2(L^a)^3 + 1}{(L^a)^2 + L^a} < 2L^a. \qquad (7)$$

Згідно (7) для знаходження першого *B*-гладкого необхідно не більше ніж $2L^a (1 + 1) = 4L^a$ пробних *x*, що відповідає радіусу просіювання $2L^a$. Оскільки така умова дійсна для всіх значень *k*, при $2L^a + 2$ значеннях *k* отримаємо не менше ніж $2L^a + 2$ *B*-гладких чисел, що достатньо для формування матриці та вирішення задачі факторизації.

Як свідчать наведені оцінки, при такому підході число пробних *x*, необхідних для факторизації, оцінюється величиною $4(L^a)^2$, що значно менше за $2(L^a)^3$. Проте в такому алгоритмі факторизації наявні додаткові операції, а саме: $2L^a + 2$ обчислення кореня з великого числа; $2L^a + 2$ формування ФБ і для кожного з елементів *p* ФБ пошук числа $0 \le t < p$, для яких $((x_0 + t)^2 - kN) \bmod p^i = 0$, де $i \ge 1$; $p^i < B$. Додаткове збільшення обчислювальної складності отримуємо і при вирішенні матриці, розмір якої збільшується вдвічі та визначає асимптотичну оцінку обчислювальної складності того ж порядку, що і для алгоритму методу QS. Тому необхідно оцінити обчислювальну складність методу MQ*k*S для випадків, коли границя гладкості *B* менша за L^a.

Алгоритм методу MQ*k*S. Будемо обирати такі параметри, як границя гладкості *B* та розмір радіусу просіювання *L*, а також визначати необхідну кількість *B*-гладких чисел, і після того виконувати їх обробку. Відтак, кроки алгоритму не передбачають діагоналізацію матриці «на ходу».

Алгоритм ***A*** методу MQ*k*S має таку послідовність кроків:

1. Для заданого *N* визначити границю гладкості *B*, число *La* елементів загальної ФБ та розмір радіусу просіювання *L*. Лічильнику *k* присвоїти значення нуль.

2. $k = k + 1$.

3. У випадках, коли k ділиться на квадрат двох чи більше різних простих чисел, перейти до кроку 2.

4. Для числа kN виконати:

4.1. Сформувати множину елементів ФБ, що відповідає kN, при відомому обмеженні на границю гладкості B, тобто визначити множину простих чисел p, що ввійдуть до поточної ФБ, де $p < B$ і символ Лежандра $\left(\frac{kN}{p}\right)=1$. Якщо кількість таких чисел Lk мала по відношенню до $La/2$, то перейти до кроку 2, а інакше — до кроку 4.2.

4.2. Визначити $x_0 = \lfloor \sqrt{kN} \rfloor + 1$, $xp = x_0$, $xm = x_0 - 1$, значення $yp = xp^2 - kN$ і $ym = kN - xm^2$.

4.3. Сформувати додаткову інформацію, на основі якої можна зменшити обчислювальну складність на кроках 5.

5. Визначати B-гладкі в інтервалі просіювання.

5.1. $c = -1$.

5.2. $c = c + 1$.

5.3. Якщо $c > L$, перейти до кроку 2, а інакше — до кроку 5.4.

5.4. Якщо $c = c_{\max}$, присвоїти: $c = 0$, $xp = xp + c_{\max}$, $xm = xm - c_{\max}$, $yp = xp^2 - kN$ та $ym = kN - xm^2$. Перейти до кроку 5.5.

5.5. $x = xp + c$.

5.6. Обчислити $y = x^2 - kN = (xp + c)^2 - kN = xp^2 - kN + 2xp\,c + c^2 = yp + 2xp\,c + c^2$.

5.7. Перевірити, чи можна подати y як добуток елементів поточної ФБ. Якщо так, то перейти до кроку 5.8, а інакше — до кроку 5.9.

5.8. Зафіксувати інформацію про B-гладке та перейти до кроку 5.9.

5.9. $x = xm - c_0$.

5.10. Обчислити $y = kN - x^2 = kN - (xm - c)^2 = kN - xm^2 + 2xm\,c - c^2 = ym + 2xm\,c - c^2$.

5.11. Перевірити, чи можна подати y як добуток елементів поточної ФБ. Якщо так, то перейти до кроку 5.12, а інакше — до кроку 5.13.

5.12. Зафіксувати інформацію про B-гладке y, а також значення k та c.

5.13. Якщо при поточному c знайдено хоча б одне B-гладке число, перейти до кроку 5.13, а інакше — до кроку 5.14.

5.14. Якщо загальна кількість знайдених B-гладких чисел більша за $La + 1$, перейти до кроку 6, а інакше — до 5.14.

6. Діагоналізувати матрицю та знайти нульовий рядок. Якщо нульовому рядку відповідає тривіальний корінь рівняння (5), замінити його іншим B-гладким за наявності, а інакше — перейти до кроку 5.2. Якщо отримано нетривіальний корінь рівняння (5), то вивести значення множників числа N і закінчити роботу алгоритму.

Реалізація алгоритму *A*. На кроці 1 алгоритму ***A*** для визначення числа *La* елементів ЗФБ, границі гладкості *B* і радіусу просіювання *Lb* пропонується використовувати такі співвідношення:

$$La = (e^{\sqrt{\ln N \ln\ln N}})^{ka\sqrt{2}/4} = (L^a)^{ka}, \quad (8)$$

$$Lb = (e^{\sqrt{\ln N \ln\ln N}})^{kb\sqrt{2}/4} = (L^a)^{kb}, \quad (9)$$

де коефіцієнти *ka* і *kb* — параметри, що використовуються при проведенні чисельних експериментів. Границя ФБ *B* — це просте число, яке в списку зростаючих значень простих відповідає номеру *La*. Кроки 2 і 3 — це робота з лічильником значень *k*. Кроки 5.1—5.5, та 5.9 визначають правила роботи для лічильника значень з області просіювання. Число *N* — це велике число, в якому перевищено обмеження для базових типів long та double. Тому для виконання арифметичних операцій слід або скористатися бібліотекою для роботи з великими числами, або представляти великі числа масивами коефіцієнтів їх розкладання за деякою основою та виконувати операції для масивів чисел.

При комп'ютерній реалізації алгоритму ***A*** використано другий підхід. При розкладанні за основою *b* великих чисел *u* і *v* у вигляді

$$u = \sum_{i=0}^{m_u} u_i b^i, \quad v = \sum_{i=0}^{m_v} v_i b^i$$

у відповідних їм масивах *U* і *V* чисел буде записано:

$$U[0] = m_u + 1,\ U[j] = u_{j-1}\ (j = 1 \div m_u + 1),$$

$$V[0] = m_v + 1,\ V[j] = v_{j-1}\ (j = 1 \div m_v + 1).$$

Тоді при обчисленні суми чисел *u* і *v* додаються відповідні значення елементів масиву, а при перевищенні сумою значення $b - 1$ від суми віднімається *b* і добавляється одиниця до наступного розряду. При $u > v$ віднімання виконується так само, але при від'ємній величині різниці значень у відповідних клітинках масиву до результату додається *b*, а від значення в наступній клітинці масиву *U* віднімається одиниця.

При множенні *u* і *v* отримуємо масив *UV* довжиною більше ніж $U[0] + V[0] + 1$, коефіцієнти якого визначаються за правилом

$$uv = \sum_{i=0}^{m_u} u_i b^i \sum_{j=0}^{m_v} v_j b^j = \sum_{t=0}^{m_u+m_v} b^i \sum_{s=0}^{t} u_s v_{t-s} = \sum_{t=0}^{m_u+m_v} b^i z_t,$$

де при $z_0 \ge b$ приймаємо значення $UV[1]$ рівним остачі від ділення z_0 на *b* ($UV[1] = z_0 \pmod b$), цілу частину від ділення z_0 на *b* додаємо до z_1: $z_1^* = z_1 + [z_0 / b]$, а при $i > 0$ $UV[i+1] = z_i^* \pmod b$, де $z_i^* = z_i + [z_{i-1}^* / b]$.

При діленні u на v необхідно шукати цілі значення частки і остачі. Для їх обчислення визначається число a типу double, $a = V[m_v + 1]\,b + V[m_v] + 1$, на яке ділилася величина $U^*[j+2]\,b^2 + U^*[j+1]\,b + U[j]$ при $j = 0 \div m_u - m_v$, де $U^*[j+2]$ та $U^*[j+1]$ — це результат віднімання від u попередніх значень частки, помноженої на v.

Для обчислення квадратного кореня з N використовується відома ітераційна формула $x_{i+1} = (x_i + N/x_i)/2$, яку можна подати у вигляді

$$x_{i+1} = x_i + \frac{y_i}{2x_i} = x_i + dx_i, \quad y_i = y_{i-1} - 2x_i dx_i - dx_i^2, \tag{10}$$

де початкове значення y_0 обчислювалося з використанням функції sqrt(). За формулою (10) при відніманні від N отриманої частки на кожній ітерації уточнювалося значення x_i до тих пір, поки $N - x_i^2$ не ставало меншим за $2x_i$.

Для роботи з великими числами обиралася деяка «зручна» основа числення, в якості якої використовувалося значення 1000 чи 1024. При цьому у масивах даних, що відповідають великому числу, в нульовому елементі масиву вказувалося значення найбільшого номера з ненульовим коефіцієнтом. Для реалізації кроку 4.1 визначалися значення символів Лежандра $\left(\frac{N}{p}\right)$, де p — просте число із загальної ФБ. Враховуючи те, що $\left(\frac{(kN)}{p}\right) = \left(\frac{N}{p}\right)\left(\frac{k}{p}\right)$, значення $\left(\frac{N}{p}\right)$ зберігалися в пам'яті протягом всього часу розрахунків, а для кожного k обчислювалися значення $\left(\frac{k}{p}\right)$, де k і p — не належать до великих чисел, що дозволяло просто обчислювати символи Лежандра $\left(\frac{kN}{p}\right)$.

Всі p, для яких $\left(\frac{kN}{p}\right) = 1$, — це елементи ФБ, визначеної для простих p, що не перевищують границю гладкості B. Їх число Lk може бути різним при різних k, але завжди менше за La. Спостерігалися випадки, коли Lk було значно менше за La. Наприклад, $Lk < 10$ при $La > 250$. У таких випадках практично ніколи не вдавалося отримати хоча б одне B-гладке число на всьому інтервалі просіювання. Тому пропонувалося не шукати B-гладкі, а збільшувати k на одиницю. Але у випадках, коли $2\,Lk > La$, виявилося, що доцільно збільшувати інтервал просіювання. Тому в залежності від k встановлювали інтервал просіювання Lb $(2Lk/La)^5$. Показник степеня п'ять був підібраний за результатами чисельних експериментів.

На кроці 4.2 обчислювалося значення кореня з kN та введено такі змінні: xp — значення пробного x, при якому $x^2 > kN$; xm — значення пробного x, при якому $x^2 < kN$; yp — значення $xp^2 - kN$; ym — значення $kN - xm^2$ — додатне число при $x^2 < kN$. Далі ці значення часто використовуються. Тому на етапі підготовки до просіювання пробних x при фіксованому kN вони подавалися як масиви розкладань за основою степенів простих чисел — елементів ЗФБ. Степені m простих p вибиралися за умов:

$$p^m > 100, \quad p^m < 20000. \tag{11}$$

При виконанні умов (11) число елементів в масивах $mpxp[i][*]$, $mpxm[i][*]$, $mpyp[i][*]$, $mpym[i][*]$ (i — порядковий номер простого p в ЗФБ), що відповідають розкладанням xp, xm, yp та ym за основою p^m не перевищували 200 клітинок пам'яті для чисел N порядку 2^{1024}. Такі масиви дозволяють відносно просто визначати дільники yp та ym, що є найбільш затратною за часом процедурою. Пошук дільників та виявлення B-гладких здійснюється так:

1. Для yp обчислити наближене значення $z_0 = \ln(yp)$ та присвоїти $z = z_0$.

2. В циклі по параметру i для елементів поточної ФБ p_i з порядковим номером j в ЗФБ виконати операції:

2.1. Обчислити $t = mpyp[j][1] + 2c\, mpxp[j][1] + c^2$.

2.2. Перевірити, чи ділиться t на p_i без остачі. Якщо ні, то перейти до аналізу наступного простого p для поточної ФБ, якщо так, то перейти до кроку 2.3.

2.3. Визначити показник m степеня p такий, що для остач від ділення t на p^m та t на p^{m+1} виконано умови: $t \,\%\, p^m = 0$, $t \,\%\, p^{m+1} > 0$.

2.4. Обчислити різницю $z_j = z - m \ln(p_i)$ та присвоїти $z = z_j$.

2.5. Якщо множину елементів поточної ФБ вичерпано, то перейти до п. 3, а інакше — до аналізу наступного простого p для поточної ФБ.

3. Якщо отримане значення z близьке до нуля, то отримано B-гладке число.

Алгоритми ***A*** реалізовано програмно мовою С для двох варіантів.

1) Для базового методу QS, коли пошук B-гладких виконується за співвідношенням (1), число елементів ФБ визначається згідно (2), а радіус інтервалу просіювання — згідно (3).

2) Для методу MQkS, коли пошук B-гладких виконується за співвідношенням (6), число елементів ФБ визначається згідно (8), а радіус інтервалу просіювання — згідно (9).

Метод QS працює в два етапи: на першому визначається множина B-гладких чисел, а на другому на їх основі визначаються нетривіальні множники N. Оскільки при використанні різних алгоритмів різною буде

множина *B*-гладких чисел, для того, щоб мати змогу порівнювати методи, вирішувалася тільки задача пошуку числа *B*-гладких, рівного $L^a + 3$ при однакових значеннях La. Додатково проводилися розрахунки методом MQ*k*S при менших значеннях La.

Вплив розміру ФБ та радіусу просіювання на час формування множини *B*-гладких в методі MQ*k*S. Для порівняння ефективності методів QS та MQ*k*S проводилися чисельні експерименти з числами *N*, які є добутком двох простих та близькі до 10^m, де $m = 10 \div 32$. У зв'язку зі значною обчислювальною складністю процедури формування *B*-гладких при кожному *m* кількість чисел *N*, для яких визначалися *B*-гладкі, обмежувалася 25. Такі числа формувалися за наступними правилами.

1. Вибиралися два випадкові числа: $r_1 = 19189$ і $r_2 = 35287$. Всі наступні визначалися за формулою $r_{i+2} = (r_{i+1} + r_i)(a_1 + a_2 i)(i \geq 0)$, де $a_1 = 1{,}075$, $a_2 = 0{,}0025$.

2. Із пари отриманих послідовних чисел $r_i\,(i = 0 \div 48)$ одне залишалося незмінним, а інше вибиралося таким, що їх добуток був максимально близьким до 10^m. Для кожної наступної пари показник степеня *m* збільшувався на одиницю, а отримана множина чисел була зростаючою послідовністю. Такі числа названо опорними.

3. Для кожного опорного числа визначалися найближчі п'ять послідовних простих, які більші або рівні опорному.

4. Значення простих чисел подавалися як сума опорного значення та приросту до нього, де прирости були малими числами. Опорні числа визначалися коефіцієнтами їх розкладання за основою 1000.

5. Кожне з 25 чисел *N* було добутком двох простих, сформованих на основі двох послідовних опорних.

6. Поточне значення $N_n = (O_1 + r_i)\ (O_2 + z_j), i = 1 \div 5,\ j = 1 \div 5,\ n = 5\,(i - 1) + j$, де O_1, O_2 — опорні значення; r_i, z_j — прирости відповідно до O_1 і O_2 такі, що $O_1 + r_i$ та $O_2 + z_j$ — прості.

Сформовані опорні значення та прирости до них при $m = 20 \div 31$ наведено в табл. 4 та використано у всіх чисельних експериментах.

У першій групі чисельних експериментів оцінювали тривалість та кількість просіяних значень пробних *x* для базового методу QS та методу MQ*k*S при пошуку $La + 3$ *B*-гладких чисел. Розмір ФБ визначали згідно (2), тобто $La = L^a$, розмір інтервалу просіювання Lb для різних значень *k* в методі MQ*k*S дорівнював L^a, а в методі QS — $(L^a)^3$.

На рис. 1 надано інформацію про відношення тривалості *T* (QS) формування множини $La + 3$ *B*-гладких чисел методом QS до аналогічної величини *T* (MQ*k*S) методом MQ*k*S, а також про відношення числа *P* (QS) просіяних *x* методом QS до аналогічного числа, отриманого методом MQ*k*S.

За отриманими результатами можна зробити висновок, що метод MQ*k*S потребує в 1,5—3,5 рази менше часу при формуванні множини *B*-гладких чисел, ніж метод QS. Це пояснюється зменшенням числа просіюваних пробних x в шість і більше разів. Слід зазначити, що обидві характеристики корелюють між собою. Враховуючи те, що розмір матриці в обох методах не змінився, обчислювальна складність методу MQ*k*S буде така ж, як і методу QS. Її суттєвого зниження можна досягнути при зменшенні розміру ЗФБ в порівнянні з L^a. Згідно з (8) при $ka < 1$ зменшуються розмір

Таблиця 4. **Прості числа, подані як опорні значення та прирости до них**

m	Опорні значення	Прирости до опорних значень				
		1	2	3	4	5
20	6 471 594 853	16	36	54	96	120
	15 452 141 593	58	76	78	106	118
21	27 749 160 899	32	42	54	92	140
	36 037 125 721	42	88	100	112	120
22	87 614 993 781	8	82	86	110	116
	114 135 715 457	2	12	14	36	54
23	274 858 909 339	34	54	94	114	130
	363 823 025 568	1	25	29	43	79
24	651 133 587 339	4	14	58	98	104
	1 535 783 162 540	53	63	83	149	219
25	2 095 629 580 239	142	160	184	248	292
	4 771 835 678 545	28	46	48	108	118
26	6 787 809 030 482	39	41	77	111	195
	14 732 294 257 385	24	78	122	158	194
27	22 126 102 809 573	8	16	34	58	76
	45 195 487 366 502	131	167	195	215	225
28	72 582 191 787 419	14	32	68	108	222
	137 774 841 923 874	89	107	119	133	137
29	239 604 396 594 260	47	81	209	293	357
	417 354 612 108 130	21	39	67	123	133
30	687 691 741 189 047	100	104	176	184	244
	1 454 139 900 343 951	16	22	130	162	190
31	2 660 737 903 883 030	101	153	219	243	329
	3 758 355 900 220 833	20	28	38	70	80

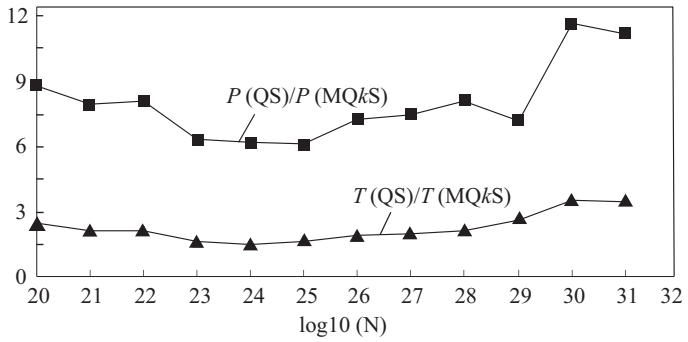

Рис. 1. Графіки відношення чисел використаних пробних x при просіюванні та тривалості формування B-гладких для методів QS та MQkS

ФБ і розмір матриці, що може зумовити загальне зниження обчислювальної складності методу MQkS по відношенню до методу QS.

Проте, як зазначено вище, зменшення розміру ФБ призводить до зменшення числа B-гладких на тому ж інтервалі просіювання, у зв'язку з чим зростає обсяг просіяних x та тривалість розрахунків. Тому у другій групі розрахунків методом MQkS визначався темп зростання тривалості роботи алгоритму при визначенні $La + 3$ B-гладких чисел. При зміні коефіцієнта ka змінювалося і значення La. В усіх експериментах було прийнято $Lb = L^a$ (табл. 5). Інформацію про середнє значення кількості просіяних x подано як показник степеня: $P = (L^a)^{kp}$. Отримані результати розрахунків

Таблиця 5. **Розмір загальної ФБ, обсяг просіяних значень та тривалість розрахунку при ka = 1; 0,95; 0,9**

m	L^a	$La = L^a$		$La = (L^a)^{0,95}$			$La = (L^a)^{0,9}$		
		kp	T, с	La	kp	T, с	La	kp	T, с
20	109	2,151	15,609	87	2,234	22,187	68	2,343	33,614
21	127	2,156	24,311	99	2,255	36,512	78	2,374	53,311
22	146	2,154	36,74	114	2,263	55,81	89	2,377	80,701
23	168	2,194	59,091	130	2,282	81,263	101	2,383	128,654
24	193	2,193	93,834	149	2,273	138,429	114	2,404	209,665
25	221	2,212	144,792	169	2,307	221,238	129	2,413	313,861
26	253	2,216	219,558	192	2,298	320,019	146	2,405	481,81
27	289	2,219	329,552	217	2,319	493,622	164	2,428	747,965
28	328	2,231	526,141	246	2,319	812,738	184	2,431	1175,217
29	373	2,251	776,085	277	2,346	1170,039	206	2,461	1726,182
30	423	2,257	1210,248	313	2,341	1814,613	231	2,45	3176,458

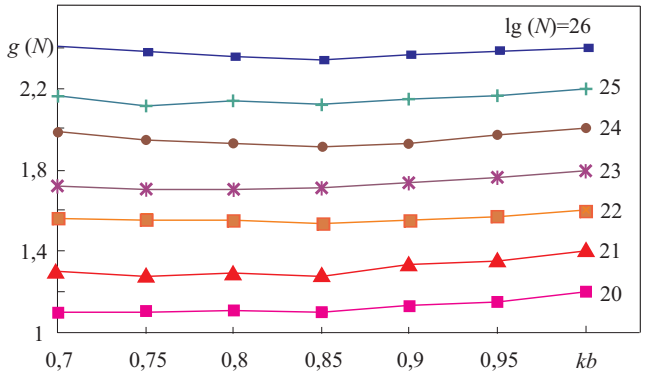

Рис. 2. Графіки $g(N) = (\ln(N) - 19)/5 + f(N, kb) / f(N, 1)$ відповідно даних табл. 5

свідчать про те, що при зменшенні значення *ka* зменшується розмір ФБ, але зростає тривалість обчислень та кількість просіяних *x*.

Попередній аналіз щодо розміщення *B*-гладких чисел показав, що їх більше при близьких до $\sqrt{N}$ значеннях пробних, що відповідає невеликому радіусу просіювання. Тому, вочевидь, зменшення тривалості формування множини *B*-гладких та кількості пробних *x* можна досягнути при зниженні радіусу просіювання. Для перевірки даної гіпотези проведено серію експериментів при $N = 10^m$, де $m = 20 \div 26$, $La = (L^a)^{0,95}$, $Lb = (L^a)^{kb}$ та зміні значення *kb* (рис. 2). Враховуючи те, що при $kb = 0,85$ в більшості випадків отримано мінімальну тривалість розрахунку, було проведено чисельні експерименти з визначення параметра *ka* для забезпечення одночасного зменшення тривалості формування множини *B*-гладких чисел і розміру ЗФБ.

У табл. 7 наведено результати для методів QS при $La = L^a$ та MQ*k*S при $La = (L^a)^{0,95}$ і $La = (L^a)^{0,9}$, де $Lb = (L^a)^{0,85}$. Аналізуючи дані, наведені в табл. 7, можна зробити висновок, що при $ka = 0,95$ і $kb = 0,85$ тривалість отримання

Таблиця 6. **Тривалість розрахунку при зміні радіуса просіювання та *ka* = 0,95 згідно (9)**

m	Тривалість $T = f(N, kb)$ роботи алгоритму **A** при *kb*						
	1	0,95	0,9	0,85	0,8	0,75	0,7
20	22,001	20,898	20,519	19,889	19,986	19,86	19,799
21	35,304	33,671	33,023	30,942	31,312	31,013	31,812
22	51,842	50,279	49,67	48,748	49,139	49,232	49,898
23	80,825	77,576	75,906	73,81	73,419	73,185	74,513
24	127,037	123,356	117,42	116,034	118,541	120,18	124,648
25	203,255	196,106	192,602	187,894	190,134	186,431	195,461
26	306,209	301,724	294,719	288,89	294,372	299,161	308,02

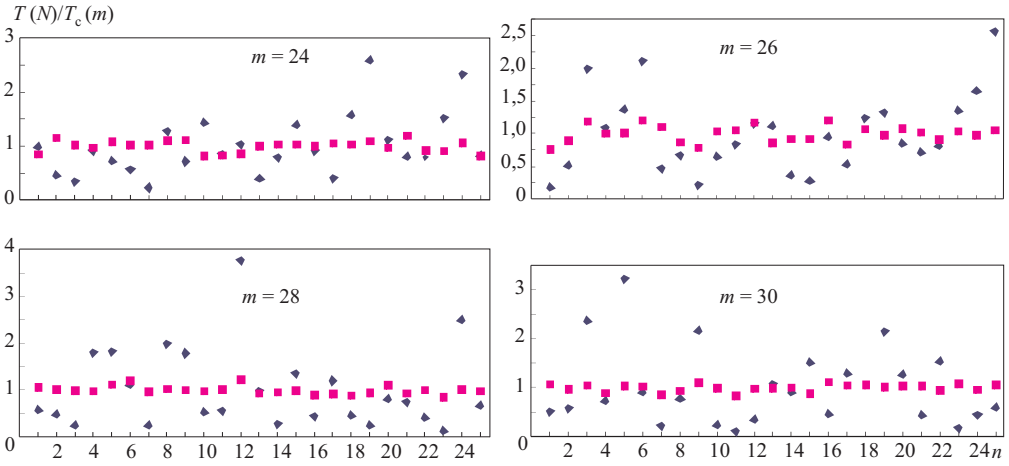

Рис. 3. Відношення $T(N)/T_c(m)$, отримані для 25 значень N_n: ◆ — метод QS; ■ — метод MQ*k*S

Таблиця 7. **Обсяг просіяних значень та тривалість розрахунку *B*-гладких для методів QS та MQ*k*S**

m	QS			MQ*k*S							
	$La = L^a$			$La = (L^a)^{0,95}$				$La = (L^a)^{0,9}$			
	L^a	*kp*	*T*, с	*La*	*Lb*	*kp*	*T*, с	*La*	*Lb*	*kp*	*T*, с
20	109	2,615	28,81	87	54	2,194	19,87	68	54	2,31	29,91
21	127	2,584	40,41	99	61	2,202	30,94	78	61	2,311	47,58
22	146	2,573	60,17	114	69	2,227	48,75	89	69	2,33	77,98
23	168	2,555	86,33	130	78	2,232	73,81	101	78	2,344	113,98
24	193	2,538	123,78	149	88	2,227	116,03	114	88	2,353	181,01
25	221	2,548	203,98	169	99	2,257	187,89	129	99	2,383	289,15
26	253	2,574	361,59	192	110	2,261	288,89	146	110	2,363	436,89
27	289	2,574	564,78	217	123	2,282	439,8	164	123	2,391	681,96
28	328	2,592	1000,66	246	138	2,283	698,26	184	138	2,392	1054,73
29	373	2,584	1586,62	277	153	2,311	1032,23	206	153	2,421	1599,94
30	423	2,663	3919,69	313	171	2,309	1583,96	231	171	2,418	2442,62
31	479	2,653	5036,85	352	190	2,318	2418,51	258	190	2,42	3791,06

множини B-гладких методом MQkS є меншою, ніж методом QS, а при N = 30 і 31 необхідний час для методу QS більше ніж вдвічі перевищує необхідний час для методу MQkS. Відтак, ці дані підтверджують можливість використання методу MQkS для факторизації великих чисел. При цьому слід зазначити, що в табл. 7 (а також в табл. 5 і 6) наведено сумарний час формування B-гладких для 25 чисел. Тому важливо оцінити можливості методу MQkS при конкретних значеннях N.

Нехай $T(N)$ — тривалість розрахунку B-гладких для конкретного N, $T_c(m)$ —середнє значення тривалості розрахунку для 25 значень N порядку 10^m. На рис. 3 наведено інформацію про відношення $T(N_n)/T_c(m)$ для методів QS і MQkS. Отже, серед різних значень N існують такі, для яких тривалість пошуку множини B-гладких методом MQkS є меншою (іноді в кілька разів), ніж відношення середніх значень тривалості пошуку для методу QS. Саме для факторизації таких чисел N доцільно використовувати метод MQkS.

Висновки

Метод QS є найшвидшим для чисел величиною до 10^{110}. В ньому найбільш затратною за часом є процедура пошуку B-гладких чисел. На її тривалість істотно впливають розмір ФБ та інтервал просіювання. Існує модифікація методу QS, відома як метод MPQS, де пошук B-гладких здійснюється для різних квадратичних функцій, в яких коефіцієнти полінома є досить великими числами і їх слід шукати. В MPQS також використовуються ФБ та інтервал просіювання, що дозволяє зменшити обчислювальну складність алгоритму пошуку множини B-гладких.

В основу запропонованого методу факторизації покладено ідеї, близькі до методу MPQS. В MQkS поліноми $X^2 - kN$, за допомогою яких шукають B-гладкі числа, мають просту структуру та будуються легко. Проте в них при кожному k використовуються інші ФБ та інтервал просіювання. Це зумовило введення поняття ЗФБ, множина елементів якої містить ФБ для довільного k.

За результатами досліджень встановлено, що метод MQkS при його реалізації згідно з алгоритмом ***A*** дозволяє отримувати достатню кількість B-гладких чисел при різному розмірі ФБ, а при ka = 0,95 та kb = 0,85 є кращим за метод QS за середніми показниками часу. Таким чином, для факторизації чисел N доцільно використовувати метод MQkS, алгоритм якого можна легко адаптувати для паралельної реалізації, розділивши операції пошуку B-гладких на окремі завдання при різних значеннях k.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Горбенко И.Д., Долгов В.И., Потий А.В., Федорченко В.Н.* Анализ каналов уязвимости системы RSA. // Безопасность информации. 1995, № 2, с. 22—26.
2. *Daniel R.L. Brown.* Breaking RSA May Be As Difficult As Factoring. [Электронный ресурс]. Режим доступа: http://www.pgpru.com/novosti /2005/1026vzlomrsabezfakto-rizacii-realennoneeffektiven. — Название с экрана.
3. *Kannan Balasubramanian, M. Rajakani.* Algorithmic strategies for solving complex problems in cryptography. // Advances in information security, privacy, and ethics (AISPE) book series. Hershey, Pennsylvania (701 E. Chocolate Avenue, Hershey, Pennsylvania, 17033, USA) : IGI Global, 2018.
4. *Quadratic* sieve. [Электронный ресурс]. Режим доступа: https://en.wikipedia.org/wiki/Quadratsc_sieve.— Название с экрана.
5. *Landquist E.* The Quadratic Sieve Factoring Algorithm.// MATH: Cryptographic Algorithms. 2001, № 488, p. 1—11.
6. *RSA* numbers. [Электронный ресурс]. Режим доступа: https://en.wikipedia.org/wiki/RSA_numbers. — Название с экрана.
7. *C. Pomerance.* Smooth numbers and the quadratic sieve. Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, MSRI Publications, 2008, № 44, p. 69—81.
8. *Vazzana A., Garth D., Erickson M.J.* Introduction to number theory. Boca Raton : Chapman & Hall/CRC, 2015.
9. *Guo V.Z., Banks W.D.* Exponential sums, character sums, sieve methods and distribution of prime numbers. Columbia, Missouri: University of Missouri, 2017.
10. *Crandall R., Pomerance C.B.* Prime numbers a computational perspective. Second ed. NY: Springer, 2010.
11. *Ишмухаметов Ш.Т.* Методы факторизации натуральных чисел. Казань: Казанский ун-т, 2011, с. 190.
12. *Sahadeo Padhye, Rajeev Anand Sahu, Vishal Saraswat.* Introduction to Cryptography. Boca Raton, FL : CRC Press, 2018, p. 45.
13. *Місько В.М.* Прискорення методу квадратичного решета на основі використання умовно *B*-гладких чисел. // Зб. наук. праць. «Системні дослідження та інформаційні технології», 2018, № 1, с. 99—106.
14. *Винничук С.Д, Місько В.М.* Прискорення методу квадратичного решета на основі використання розширеної факторної бази та формування достатньої кількості *B*-гладких чисел // Зб. наук. праць. «Information technology and security», 2017, с. 67—71.
15. *Vynnychuck S., Misko V.* Acceleration analysis of the quadratic sieve method based on the online matrix solving. // Mathematics and cybernetics — applied aspects, 2018. DOI: 10.15587/1729-4061.2018.133603
16. *Silverman R.D.* The multiple polynomial quadratic sieve // Math. Comp. 1987, Vol. 48, No. 177, p. 329—339.
17. *Breitenbacher D., Homoliak I., Jaros J., Hanacek P.* Impact of Optimization and Parallelism on Factorization Speed of SIQS// Journal of Systemics, 2016, Vol. 4, No. 3 p. 51—58.

Отримано 01.10.18

REFERENCES

1. Gorbenko, I.D., Dolgov, V.I., Potiy, A.V. and Fedorchenko, V.N. (1995), "Channel analysis of the RSA system vulnerability", *Bezopasnost informatsii*, no. 2, pp. 22-26.
2. Brown, D.R.L. (2005), Breaking RSA May Be As Difficult As Factoring, available at: http://www.pgpru.com/novosti /2005/1026vzlomrsabezfaktorizaciirealennoneeffektiven.
3. Kannan Balasubramanian and Rajakani, M. (2018), Algorithmic strategies for solving complex problems in cryptography. Advances in information security, privacy, and ethics (AISPE) book series, Hershey, Pennsylvania (701 E. Chocolate Avenue, Hershey, Pennsylvania, 17033, USA), IGI Global.
4. Quadratic sieve, available at: https://en.wikipedia.org/wiki/Quadratic_sieve.
5. Landquist, E. (2001), "The Quadratic Sieve Factoring Algorithm", *MATH Cryptographic Algorithms*, no. 488, pp. 1-11.
6. RSA numbers, available at: https://en.wikipedia.org/wiki/RSA_numbers.
7. Pomerance, C. (2008), "Smooth numbers and the quadratic sieve. Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography", *MSRI Publications*, no. 44, pp. 69- 81.
8. Vazzana, A., Garth, V. and Erickson, V. (2015), Introduction to number theory, Boca Raton, Chapman & Hall/CRC.
9. Guo, V.Z. and Banks, W.D. (2017), Exponential sums, character sums, sieve methods and distribution of prime numbers, University of Missouri, Columbia, Missouri.
10. Crandall, R. and Pomerance, C.B. (2010), Prime numbers a computational perspective (Second ed.). New York, NY, Springer.
11. Ishmukhametov, Sh.T. (2011), *Metody faktorizatsii naturalnykh chisel* [Methods of natural numbers factorization], Kasanskiy Universitet, Kasan, Russia.
12. Sahadeo Padhye, Rajeev Anand Sahu and Vishal Saraswat (2018), Introduction to Cryptography, Boca Raton, FL, CRC Press.
13. Misko, V. (2018), "Acceleration of the method of a quadratic sieve based on the use of conditionally *B*-smooth numbers", *Zbirnyk naukovykh prats* «System research and information technologies», no. 1, pp. 99-106.
14. Vinnichuk, S. and Misko, V. (2017), "Acceleration of the quadratic sieve method based on the use of an expanded factor base and the formation of a sufficient number of *B*-smooth numbers", *Zbirnyk naukovykh prats* «Information technology and security», pp. 67-71.
15. Vynnychuck, S. and Misko, V. (2018), Acceleration analysis of the quadratic sieve method based on the online matrix solving. Mathematics and cybernetics — applied aspects, DOI: 10.15587/1729-4061.2018.133603.
16. Silverman, R.D. (1987), "The multiple polynomial quadratic sieve", *Math. Comp.*, Vol. 48, no. 177, pp. 329-339.
17. Breitenbacher, D., Homoliak, I., Jaros, J. and Hanacek, P. (2016), "Impact of Optimization and Parallelism on Factorization Speed of SIQS", *Journal of Systemics*, Vol. 4, no. 3, pp. 51-58.

Received 01.10.18

С.Д. Винничук, В.Н. Мисько

МЕТОД МНОЖЕСТВЕННОГО КВАДРАТИЧНОГО
K-РЕШЕТА ЦЕЛОЧИСЛЕННОЙ ФАКТОРИЗАЦИИ

Предложена модификация метода квадратичного решета (QS), в которой при поиске *B*-гладких чисел используются полиномы $X^2 - kN$. В отличие от методов QS и множественного полиномиального квадратичного решета (MPQS) в предлагаемом методе множественного квадратичного *k*-решета (MQ*k*S) используется общая факторная база (ФБ), которая детализируется при каждом значении *k*. В алгоритме учтено, что число *B*-гладких относительно больше при меньших значениях чисел из интервала просеивания. Это подтверждено данными численных экспериментов. Описаны шаги предлагаемого алгоритма и идеи их реализации. На основании численных экспериментов показано, что с помощью метода MQ*k*S можно достичь уменьшения в среднем времени формирования множества *B*-гладких по сравнению с методом QS при меньшем размере ФБ.

К л ю ч е в ы е с л о в а: целочисленная факторизация, метод квадратичного решета, множественное решето.

S.D. Vynnychuk, V.M. Misko

METHOD OF MULTIPLE QUADRATIC K-SILVE INTEGER FACTORIZATION

A modification of the quadratic sieve method (QS) is proposed, in which the polynomials $X^2 - kN$ are used in the search for *B*-smooth numbers. In contrast to the QS and multiple polynomial quadratic sieve (MPQS) methods, the proposed multiple quadratic *k*-sieve method (MQ*k*S) uses a common factor base (FB), which is detailed for each k value. The algorithm takes into account that the number of *B*-smooth is relatively larger with smaller values of the numbers from the sifting interval. This is confirmed by the data of numerical experiments. The steps of the proposed algorithm and their implementation are described. Based on numerical experiments, it was shown that using the MQ*k*S method, it is possible to achieve a decrease in the average time of formation of the *B*-smooth set compared to the QS method with a smaller size of FB.

K e y w o r d s: integer factorization, quadratic k-sieve method, multiple sieve.

ВИННИЧУК Степан Дмитрович, д-р техн. наук, зав. відділом Ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. В 1977 р. закінчив Чернівецький державний університет. Область наукових досліджень — моделі, методи і програмні засоби для аналізу систем рідини, що стискається та не стискається, теорія алгоритмів.

МІСЬКО Віталій Миколайович, аспірант Ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. В 2013 р. закінчив Ін-т спеціального зв'язку і захисту інформації НТУУ «КПІ». Область наукових досліджень — чисельні методи та алгоритми факторізації.