УДК 004.021:056.55

ПРОТОКОЛ ДІФФІ–ХЕЛЛМАНА НА МНОЖЕНІ СИНГУЛЯРНИХ ПРОСТИХ ЧИСЕЛ

А. Я. Білецький, д-р техн. наук, проф.; ***О. І. Семенюк***

Національний авіаційний університет

abelnau@ukr.net

Введено клас сингулярних простих чисел, на основі яких пропонується алгоритм істотного скорочення витрат машинного часу, що потрібен на вибір прийнятних значень утворюючих елементів для протоколів Діффі–Хеллмана.

Ключові слова: протокол формування секретних ключів, прості числа, сингулярні прості числа.

Introduced the class of the singular prime numbers, based on which proposed the algorithm of significantly reduce computing time spent on the choice of suitable values for the Diffie–Hellman protocols.

Keywords: protocol of forming secret keys, simple numbers, singular simple numbers.

Вступ і постановка завдання дослідження

Опублікування Уітфілдом Діффі і Мартіном Хеллманом у 1976 р. статті [1] знаменувало початок ери несиметричної (двоключової) криптографії.

Запропонований авторами протокол обміну даними в каналах зв'язку (мережах), що отримав назву «протокол Діффі–Хеллмана» (скорочено DH-протокол), забезпечує формування таємного ключа *K*, загального для двох легалізованих абонентів мережі (Аліси і Боба) і призначеного для використання в алгоритмах симетричного шифрування. Генерація таємного ключа *K* здійснюється у відкритих каналах зв'язку, незахищених від прослуховування супротивником (Євою), але захищених від підміни переданої інформації.

Суть DH-протоколу полягає в такому. Абонентам мережі Алісі та Бобу передбачаються відомими відкриті ключі протоколу, як такі використовуються велике просте число p і примітивний елемент q поля Галуа $GF(p)$.

Примітивний елемент q, як і p, рекомендується вибирати також достатньо великим. Аліса генерує випадковий таємний показник x, розраховує число $A = q^x \pmod p$ і посилає його Бобу.

Аналогічним чином Боб генерує випадковий таємний показник y, розраховує число $B = q^y \pmod p$ і посилає його Алісі. Після цього абоненти мережі підносять отримані від партнера числа в свої таємні степені й приводять їх до залишку за модулем p.

У результаті виконання описаних операцій у Аліси і Боба утворюється однаковий таємний ключ *K*, у силу того, що

$$B^x = q^{yx} \pmod p = A^y = q^{xy} \pmod p, \qquad (1)$$

оскільки $yx \equiv xy$.

Противник Єва, перехопивши повідомлення A і B, якими обмінюються легалізовані абоненти мережі, не в змозі обчислити ключ *K*, оскільки стикається з практично нерозв'язною в даний час проблемою дискретного логарифмування, якщо тільки відкриті ключі p і q вибрані досить великими. Рекомендованими значеннями p і q є двійкові числа, розрядність яких дорівнює 1, 2 і навіть 4 Кбіт. Настільки великі розміри простих чисел p є причиною значних складнощів, які виникають при синтезі примітивних елементів q DH-протоколу. У даній роботі ставиться завдання розроблення досить ефективного алгоритму скорочення витрат машинного часу, пов'язаного з вибором утворюючих елементів q протоколів Діффі–Хеллмана. Алгоритм заснований на застосуванні нового класу так званих *сингулярних простих чисел* (СПЧ).

Статистика порядків елементів поля *GF(p)*

Множина Ω ненульових елементів поля $GF(p)$ потужності $p-1$ складається з підмножини Q примітивних елементів q і підмножини $\overline{Q}$ елементів $\bar{q}$, які не є примітивними, тобто не належать Q.

Примітивними є такі елементи (числа) q поля $GF(p)$, послідовність степенів яких по mod p формує послідовність максимальної довжини (*m*-послідовність), покриваючи всі ненульові елементи поля [2]. Найважливішою характеристикою елементів ω множини Ω є їх порядок. *Порядком*, позначуваним $ord\,\omega$, елемента $\omega \in \Omega$ поля $GF(p)$ є таке мінімальне значення показника *e*, за якого $\omega^e \pmod p = 1$.

Послідовність степенів елемента ω, починаючи з нульової степені, для якої $\omega^0 = 1$, утворює *циклічну групу*, що позначається $\langle\omega\rangle$, порядку *e*. Цілком очевидно, що примітивні елементи q поля $GF(p)$ породжують *мультиплікативні групи* $\langle q\rangle$ *максимального порядку* (МГМП). Це означає, зокрема, що $\forall q \in Q \Rightarrow ord\ q = p-1$. Як випливає зі співвідношення (1), на утворюючі елементи q і показники x і y протоколу Діффі–Хеллмана повинні бути накладені, принаймні, такі обмеження. По-перше, елемент q, як уже було зазначено вище, слід вибирати з підмножини Q примітивних елементів поля $GF(p)$. І, по-друге, показники x і y не повинні перевищувати значення $ord\ q-1$, яке дорівнює $p-2$.

Коротко, спираючись на числові приклади, пояснимо причини, що зумовлюють необхідність наведених обмежень.

Отже, нехай $p = 19$ і, відтак, $ord\ q = 18$. Поле $GF(19)$ включає 18 ненульових елементів, з яких шість примітивні. Такими є числа 2, 3, 10, 13, 14 і 15, обчислені за допомогою програми, інтерфейс якої показано на рис. 1.

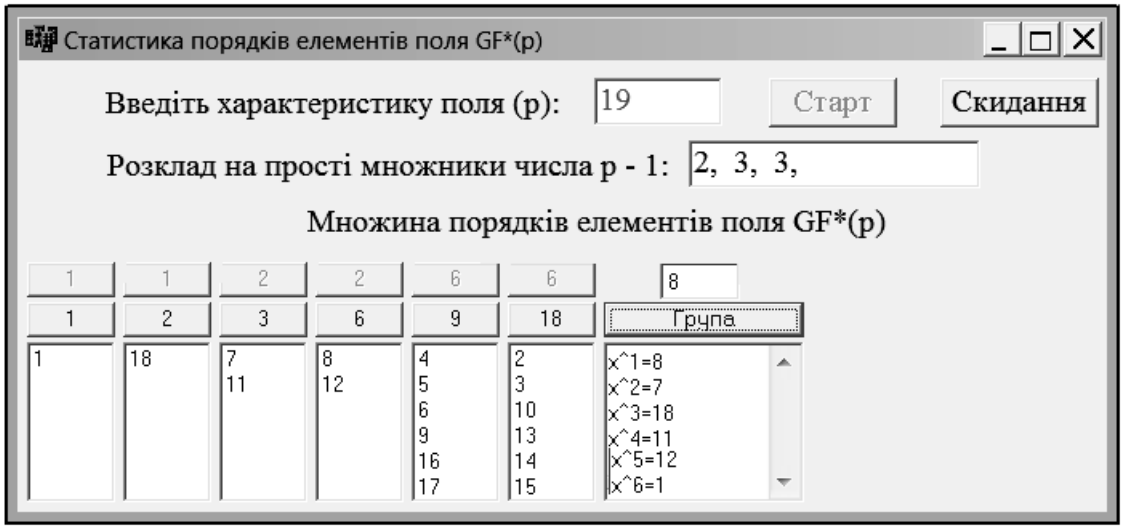

Рис. 1. Інтерфейс програми «Статистика порядків елементів поля $GF(p)$» і результати розрахунку для $p = 19$

На середніх клавішах інтерфейсу наведені значення порядків ненульових елементів поля $GF^*(19)$, над ними — число елементів даного порядку, а в нижніх вікнах — список цих елементів. Мультиплікативна група, для прикладу, розрахована щодо створюючого елемента $\omega = 8$, який вставлений у вікно над клавішею «Група» інтерфейсу. Поле $GF^*(p)$, тобто поле $GF(p)$, за винятком його нульового елемента, називають також *мультиплікативною групою максимального порядку*, або просто *мультиплікативною групою поля* $GF(p)$.

Виберемо як утворюючий елемент (УЕ) DH-протоколу будь-який примітивний елемент *q* поля $GF(19)$. А тепер припустимо, що значення одного з показників, наприклад, x збігається з порядком примітивних елементів, тобто $x = 18$ (або кратний 18). Це призводить до того, що незалежно від величини *q*, отримаємо $q^x = q^{18} = q^{ord\ q} = 1$. У такому випадку Єва, перехопивши повідомлення $A = 1$, прийде до однозначного висновку про те, що показник $x = 18$. Наслідком даного висновку є те, що Єві стає відомим таємний ключ K протоколу Діффі–Хеллмана, оскільки $K = B^x = B^{18} = B$. Якщо ж $x > ord\ q$, то представивши x співвідношенням $x = m \cdot ord\ q + x$, де m — натуральне число, а x — залишок числа x за модулем p, менший ніж $ord\ q$, отримаємо, що $q^x = q^x$, оскільки

$q^{m \cdot ord\, q} \equiv 1$. Отже, вибирати значення x, більше ніж $ord\, q - 1$, немає сенсу. Це, у будь-якому разі втрачає сенс як утворюючий елемент DH-протоколу вибирати елемент, який не є примітивним елементом поля $GF(p)$. Насправді, припустимо, що утворюючим обраний елемент $\theta = 8$, який не належить підмножині Q, а показник $x = 17$. Порядок елемента $\theta = 8$ у полі $GF(19)$ дорівнює шести, тобто $ord\, \theta = 6$. Отже, показник x можна представити у вигляді $x = 2 \cdot ord\, \theta + 5$, що призводить до співвідношення $\theta^x = \theta^{17} \equiv \theta^5$, оскільки $\theta^{2 \cdot ord\, \theta} \equiv 1$. Таким чином підтвердили доцільність обмежень, які повинні накладатись на утворюючі елементи q протоколу Діффі–Хеллмана.

Сингулярні прості числа

Як було зазначено вище, рекомендовані розміри простих чисел p у DH-протоколах досягають великих значень, складаючи кілька Кбіт. У зв'язку з цим можуть виникнути певні складнощі, пов'язані з вибором примітивних утворюючих елементів q. Покажемо суть даної проблеми на прикладі простого числа $p = 64081$. Обчислені за допомогою згадуваної вище програми «Статистика» множина порядків ненульових елементів поля $GF^*(p)$ і відповідні їм (порядкам) частоти зведені в табл. 1.

Як випливає з табл. 1 відносна частота примітивних елементів аналізованого поля $GF^*(p)$, в якому $p = 64081$, становить порядку 0,26. Для великих значень p частість примітивних елементів може досягати істотно менших величин, що і є причиною проблем, що виникають під час пошуку утворюючих елементів у DH-протоколі. Нижче буде запропоновано спосіб вибору характеристик p поля $GF^*(p)$, який гарантує досягнення частості примітивних елементів на рівні 0,5. Цей спосіб заснований на використанні так званих сингулярних (особливих) простих чисел.

Сингулярними будемо називати такі прості числа p, для яких нетривіальними дільниками числа $p - 1$ є лише числа 2 і $(p-1)/2$. Згідно з визначенням, дільник $(p-1)/2$ також має бути простим числом, позначимо його p^*, тобто повинна виконуватися умова

$$p = 2p^* + 1,$$

причому як p, так і p^* — прості числа.

У табл. 2 наведено значення перших 144 сингулярних простих чисел. Порядковий номер k СПЧ у таблиці визначається сумою номерів її стовпця i і значення j у відповідному рядку табл. 2, тобто $k = i + j$.

Таблиця 1

Статистичні характеристики елементів поля GF^*(64081)

№	Порядок / Частота	№	Порядок / Частота	№	Порядок / Частота	№	Порядок / Частота	№	Порядок / Частота	№	Порядок / Частота
1	1 / 1	11	15 / 8	21	60 / 16	31	267 / 176	41	1335 / 704	51	5340 / 1408
2	2 / 1	12	16 / 8	22	72 / 24	32	356 / 176	42	1424 / 704	52	6408 / 2112
3	3 / 2	13	18 / 6	23	80 / 32	33	360 / 96	43	1602 / 528	53	7120 / 2816
4	4 / 2	14	20 / 8	24	89 / 88	34	445 / 352	44	1780 / 704	54	8010 / 2112
5	5 / 4	15	24 / 8	25	90 / 24	35	534 / 176	45	2136 / 704	55	10680 / 2816
6	6 / 2	16	30 / 8	26	120 / 32	36	712 / 352	46	2670 / 704	56	12816 / 4224
7	8 / 4	17	36 / 12	27	144 / 48	37	720 / 192	47	3204 / 1056	57	16020 / 4224
8	9 / 6	18	40 / 16	28	178 / 88	38	801 / 528	48	3560 / 1408	58	21360 / 5630
9	10 / 4	19	45 / 24	29	180 / 48	39	890 / 352	49	4005 / 2112	59	32040 / 8448
10	12 / 4	20	48 / 16	30	240 / 64	40	1068 / 352	50	4272 / 4272	60	64080 / 16896

Таблиця 2

Сингулярні прості числа

$j \setminus i$	1	2	3	4	5	6	7	8	9	10	11	12
0	7	11	23	47	59	83	107	167	179	227	263	347
12	358	383	467	479	503	563	587	719	839	863	887	983
24	1039	1187	1283	1307	1319	1367	1439	1487	1523	1619	1823	1907
36	2027	2039	2063	2099	2207	2447	2459	2579	2819	2879	2903	2963
48	2999	3023	3119	3167	3203	3467	3623	3779	3803	3863	3947	4007
60	4079	4127	4139	4259	4283	4547	4679	4703	4787	4799	4919	5087
72	5099	5387	5399	5483	5507	5639	5807	5879	5927	5939	6047	6599
84	6659	6719	6779	6827	6899	6983	7079	7187	7247	7523	7559	7607
96	7643	7703	7727	7823	8039	8147	8423	8543	8699	8747	8783	8819
108	8963	9467	9587	9743	9839	9887	10007	10079	10103	10163	10343	10463
120	10559	10607	10667	10799	10883	11003	11279	11423	11483	11699	11807	12107
132	12203	12227	12263	12347	12527	12539	12647	12659	12899	12983	13043	13103

Звернемо увагу на такий момент. Просте число $p=5$ не включено до таблиці СПЧ, незважаючи на те, що $(p-1)/2$ є простим числом, рівним 2. Таке рішення має просте обґрунтування. Насправді, для будь-якого СПЧ число $p-1$ повинно мати чотири дільники, два з яких дорівнюють 2 і $(p-1)/2$, а решта два — тривіальні дільники 1 і $p-1$. Водночас простому числу $p=5$ відповідають три дільники числа $p-1$; а саме, дільники 1, 2 і 4, оскільки дільник 2 збігається з дільником $(p-1)/2$, що порушило повноту наведеного вище визначення СПЧ. На цій підставі число 5, як і 3, не включені до складу СПЧ.

Просте поле $GF(p)$ включає $p-1$ ненульових елементів від 1 до $p-1$. Порядок елемента 1 дорівнює 1, тобто $ord\,1=1$, тоді як $ord\,(p-1)=2$. Насправді, нехай елемент a поля $GF(p)$ дорівнює $p-1$. Маємо $a^0=1$, $a^1=p-1$ і, нарешті,

$$a^2=(p-1)\cdot(p-1)=(p^2-2p+1)\,(\mathrm{mod}\ p)=1.$$

Отже, порядок елемента $a=p-1$ дорівнює двом. Мультиплікативну групу максимального порядку, породжувану тим чи іншим примітивним елементом q поля $GF(p)$, для невеликих значень p зручно відображати у вигляді спрямованого графа. На рис. 2 представлений такий граф для характеристики поля $p=11$. Усередині кружечків розміщені елементи групи, по зовнішньому контуру розташовані порядки відповідних елементів графа, а в середині — степені примітивного утворюючого елемента МГМП $q=2$.

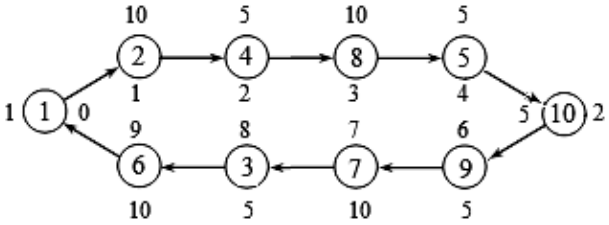

Рис. 2. Граф МГМП поля $GF(11)$ над УЕ $q=2$

Принциповими тут (на графі) є такі два моменти — ліва вершина графа за визначенням завжди дорівнює 1, а права — значенню $p-1$.

Нехай p — сингулярне просте число. Позначимо $a=a^{(p-1)/2}\,(\mathrm{mod}\ p)$. Тоді для будь-якого елемента $a\in 2, p-2$, якщо a — непримітивний елемент, то $a=1$; якщо a — примітивний елемент, то $a=p-1$, тобто

$$ord\ a=\begin{cases}(p-1)/2, & \text{якщо } a=1,\\ p-1, & \text{якщо } a=p-1.\end{cases} \qquad (2)$$

Результати роботи програми «Статистика» для СПЧ $p=64019$, найближчого (знизу) до характеристики поля $p=64081$, показано на рис. 3.

Як видно з цього рисунка, множина елементів поля $GF^*(64019)$ включає чотири групи підмножин, порядок яких дорівнює 1, 2, 32009 та 64018 відповідно. Особливість елементів простого поля Галуа, характеристика якого p є СПЧ, полягає в тому, що довільний елемент порядку $(p-1)/2$ породжує групу того самого порядку. При цьому потужність множини елементів порядку $(p-1)/2$, як і потужність множини елементів порядку $p-1$, дорівнює $(p-3)/2$.

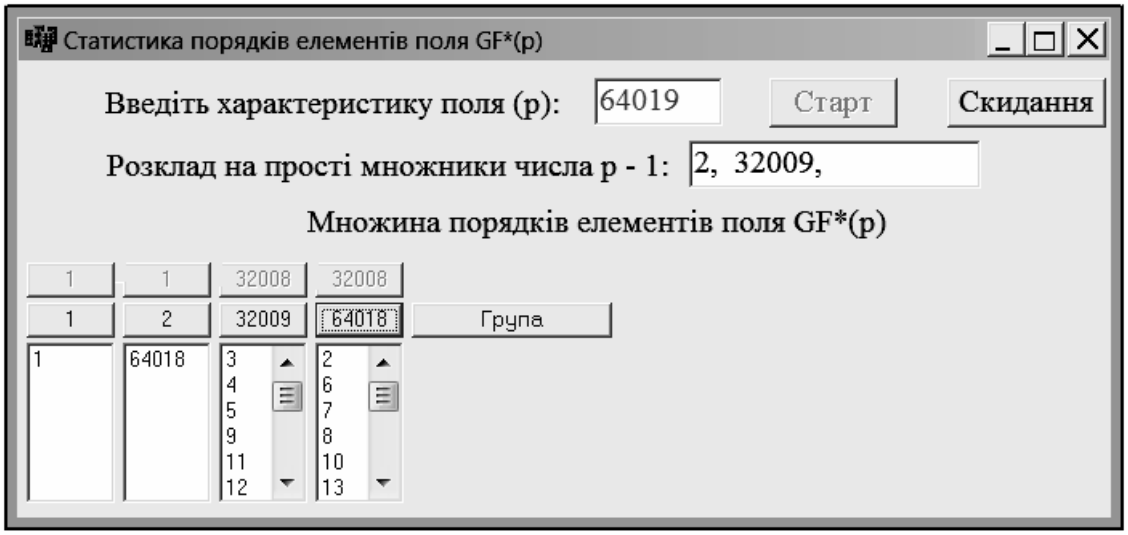

Рис. 3. Множина порядків елементів поля $GF^*(p)$ над СПЧ $p = 64019$

Спираючись на наведені властивості поля $GF(p)$ над СПЧ p і систему рівнянь (2), можна запропонувати досить простий алгоритм формування підмножин елементів поля, порядки яких визначаються значеннями $(p-1)/2$ і $p-1$ відповідно.

Суть алгоритму полягає в такому. Нехай вибрано деякий СПЧ p. Послідовно перебираючи числа $a = 2, 3, \ldots$, знайдемо таке його мінімальне значення $a = \theta$, для якого виконується умова $\theta^{(p-1)/2} \pmod p = 1$. Це, згідно зі співвідношенням (2), буде означати, що θ є мінімальним утворюючим елементом групи порядку $(p-1)/2$. Порядок усіх елементів даної групи, крім тривіального елемента 1, також дорівнює $(p-1)/2$. Виключаючи з множини чисел $\overline{2, p-2}$ елементи групи, породженої утворюючим елементом θ, отримаємо підмножину Q примітивних елементів q поля $GF(p)$. Тим самим завдання, що пов'язане з вибором утворюючого елемента (ОЕ) q протоколів Діффі–Хеллмана, стає досить легко вирішуваним.

Синтез сингулярних простих чисел

Нижче пропонуються рекомендації щодо вибору сингулярних простих чисел p, які, як зазначено у вступі, повинні бути великими числами, щоб виключити можливість злому супротивником протоколу Діффі–Хеллмана. Формування прийнятних значень p здійснюється у такій послідовності. На першому етапі слід вибрати непарне число ρ^* і функціонально пов'язане з ним число $\rho = 2\rho^* + 1$, яке також є непарним. Після цього можна переходити до перевірки простоти цієї пари чисел. Відомо велике число тестів простоти.

Найбільш простим з них є *тест Ферма* [3], заснований на *малій теоремі Ферма* [4], згідно з яким число ρ є простим, якщо воно задовольняє порівнянню

$$a^{\rho-1} \equiv 1 \pmod \rho, \qquad a \in \overline{2, \rho-1}. \tag{3}$$

Співвідношення (3) є необхідною, але далеко не достатньою ознакою простоти числа ρ. Справа в тому, що існують такі цілі ρ, які називаються *псевдопростими числами* [3], що мають деякі властивості простих чисел, будучи, тим не менше, складовими числами.

Псевдопростими, наприклад, є числа Кармайкла [5] з підстави $a = 2$, що утворюють послідовність 341, 561, 645, 1105, 1387, 1729, …, за основою $a = 3$ — числа 91, 121, 286, 671, 703, 849 і т. д.

Якщо порівняння (3), яке проводиться, як правило, за основою $a = 2$, не підтверджується хоча б для одного числа з пари ρ^* і ρ, то підбирають чергову пару непарних чисел. Після того, як знайдена пара ρ^* і ρ, яка задовольняє порівнянню (3), переходять до додаткового тестування простоти цих чисел.

Гарантовано надійним тестом є *перебір дільників*, який зводиться до повного перебору всіх можливих потенційних дільників. Зазвичай перебір дільників полягає в переборі всіх простих чисел від двох до кореня квадратного з числа, що тестується.

Якщо виявиться, що ρ^* або ρ буде кратним перебраному дільнику, то пара чисел, що тестується на простоту, бракується і процес підбору СПЧ триває над новою парою непарних чисел.

Слід зазначити, що в практичних завданнях даний алгоритм (перебір дільників) тестування простоти застосовується не часто через його велику асимптотичну складність, але його застосування виправдане в разі, якщо перевіряються відносно невеликі числа, оскільки даний алгоритм досить легко реалізується.

Висновки

Сингулярні прості числа p характеризуються тією властивістю, що мультиплікативні групи $GF^*(p)$, породжувані СПЧ p, мають мінімальний набір нетривіальних дільників.

Такими дільниками є числа 2 і $p* = (p-1)/2$. Якщо виключити зі сукупності елементів групи $GF^*(p)$ їх крайні значення 1 і $p-1$, то елементи, що залишилися, утворюють дві рівнопотужні підмножини Q і $\overline{Q}$.

Підмножина Q включає повний набір примітивних елементів q поля $GF(p)$. Підмножина $\overline{Q}$ складається з елементів, порядок яких дорівнює $(p-1)/2$, причому будь-який елемент цієї підмножини породжує мультиплікативну групу, яка крім одиниці містить усі елементи підмножини $\overline{Q}$.

Виключаючи з множини елементів поля $GF^*(p)$ елементи підмножини $\overline{Q}$ та 1, отримуємо підмножину Q примітивних q елементів поля $GF(p)$. Відзначені властивості сингулярних простих чисел дають можливість істотно скоротити витрати машинного часу, пов'язані з підбором примітивних елементів q у протоколах Діффі–Хеллмана.

ЛІТЕРАТУРА

1. *Diffe W.* New Directions in Cryptography / W. Diffe, V. E. Hellman // IEEE Transact. On Information Theory, V. IT-22, no. 6, Nov, 1976. — P. 644–654.

2. *Лидл Р.* Конечные поля / Р. Лидл, Г. Нидеррайтер. — Т. 1. — М. : Мир, 1988. — 432 с.

3. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. — М. : МЦНМО, 2003. — 328 с.

4. *Гиндикин С. Г.* Малая теорема Ферма // Квант / С. Г. Гиндикин. — 1972. — № 10.

5. *Числа Кармайкла*. — [Электронный ресурс]. — Режим доступа : Википедиа.

Стаття надійшла до редакції 11.12.2012.