УДК 519.674
https://doi.org/10.47533/2024.1606-146X.21

У. К. ТУРУСБЕКОВА[1]*, М. Ә. БЕРСҰҒІР[2]

[1]Учреждение «Esil University», Астана, Казахстан,
[2]Казахский национальный педагогический университет имени Абая, Алматы, Казахстан

ИССЛЕДОВАНИЕ АЛГОРИТМА СИЛЬВЕРА-ПОЛИГА-ХЕЛЛМАНА В ЗАДАЧАХ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

В данной работе описана постановка задачи дискретного логарифмирования, которая является важной математической проблемой. Проанализирован алгоритм вычисления дискретного логарифмирования Сильвера-Полига-Хеллмана и указаны его недостатки, возникающие из-за использования чисел специального вида, называемых гладкими. Указана проблема, которая возникает при поиске гладких простых чисел большой разрядности. Процесс поиска таких чисел замедляет алгоритм Сильвера-Полига-Хеллмана, кроме того. неизвестно возможно ли найти гладкие простые числа необходимой разрядности, ведь их количество среди простых чисел чрезвычайно мало, что ставит под вопрос эффективность использования алгоритма. Введено понятие гладкого простого числа, предложена классификация в зависимости от роста подряд расположенных множителей на идеально гладкие и частично гладкие простые числа. Проанализированы первые десять миллионов простых чисел на гладкость, среди которых идеально гладких обнаружено несколько десятков. Показано, что для поиска гладких простых чисел и анализа их свойств необходимо знать, как распределены простые числа в зависимости от количества простых сомножителей. Приведены результаты распределения первых десяти миллионов простых чисел и выдвинуты предположения о возможных законах распределения. Приведена проблема построения меры гладкости, которая должна быть рассмотрена в зависимости от разницы смежных сомножителей и их степеней.

Ключевые слова: *дискретный логарифм, простое число, гладкое простое число, первообразный корень, факторизация.*

Введение. Задача дискретного логарифмирования является одной из фундаментальных математических задач. На данный момент не существует эффективных алгоритмов вычисления дискретного логарифма. Это стало основой для создания криптографических алгоритмов с открытым ключом в начале 80-х годов, которые широко используются по сей день.

Основная идея алгоритмов с открытым ключом состоит в том, чтобы найти некоторое легко выполняемое на этапе шифрования математическое преобразование, которое было бы трудно отменить без знания секретной информации. Такое преобразование является односторонней функцией [1]. Эти функции включают в себя функцию дискретного возведения в степень, и для ее обращения требуется вычислить дискретный логарифм.

Для мультипликативных групп конечного поля и для групп, подобных эллиптическим кривым, не существует эффективных алгоритмов полиномиальных вычислений. Большинство методов имеют экспоненциальную или подэкспоненциальную сложность. Однако в случае реализации эффективных алгоритмов вычисления дискретного логарифма все криптографические системы, основанные на нем, станут непригодными. До сих пор существование такого алгоритма является открытым вопросом.

* E-mail корреспондирующего автора: umut.t@mail.ru

В работах [2], [3] рассматривается быстрый алгоритм, в котором используется определенный тип чисел, называемый “гладким”. Этот алгоритм обещает полиномиальную сложность, в случае, когда вычеты производятся по модулю простого гладкого числа, следовательно, возникает вопрос об эффективном нахождении таких чисел, и распределении этих чисел среди простых чисел, поскольку в прикладных аспектах криптографии это – числа большой разрядности. Однако четкого определения понятия гладкости не существует. Другой проблемой является поиск чисел такого типа. Далее в статье будет рассмотрен алгоритм, предложенный Сильвером, Полигом и Хеллманом, а также предложена классификация гладких чисел и представлено их распределение.

Материалы и методы. Задача дискретного логарифмирования рассматривается в кольце вычетов по модулю простого числа $(Z/mZ)^*$. Задача состоит в том, чтобы найти x, $0 \le x < p-1$, удовлетворяющее следующему сравнению:

$$a = b^x \pmod p, \tag{1}$$

где a, b, p известны, p-1является гладким (все его делители малы) и известны все его разложения q_i на простые делители $p-1 = \prod_{i=1}^{k} q_i^{\alpha_i}$ [6]. В то же время в работах [3,4] предполагается, что b является первообразным корнем по модулю p. Это означает, что вместе со своим классом вычетов он генерирует группу $(Z/pZ)^*$ [5]. Однако следует иметь в виду, что при такой формулировке алгоритм является лишь частным случаем решения дискретного логарифмирования. Также его использование требует существования алгоритмов нахождения гладких чисел.

Алгоритм из [3] содержит следующие шаги:

1. Для каждого простого делителя q вычисляются значения $r_{q_i,j} = b^{\frac{j(p-1)}{q_i}}$, где $j = \overline{(0, q_i - 1)}$. Для построения b большей степени используется метод последовательного возведения в квадрат [2].

2. Предполагается, что $x \equiv x_0 + x_1 q_i + ... + x_{\alpha_i - 1} q_i^{\alpha_i - 1} \pmod p$, где $x_i = \overline{(0, q_i - 1)}$. Чтобы найти x_0, вычисляется $a^{\frac{p-1}{q_i}} = b^{\frac{x(p-1)}{q_i}} = b^{\frac{x_0(q-1)}{p}} = r_{q_i, x_0}$. Тогда $x_0 = j$, если $a^{\frac{p-1}{q_i}} = r_{q_i, j}$.

3. $a_k^{\frac{p-1}{q_i^{k+1}}} = b^{\frac{(x_k + x_{k+1} q_i)(p-1)}{q_i}} = b^{\frac{x_k(p-1)}{q_i}} = r_{q_i, x_k}$ для каждого $k = \overline{(1, \alpha_i - 1)}$, находим $x_k = j$, если $a_k^{\frac{p-1}{q_i^{k+1}}} = r_{q_i, j}$.

4. По завершении используется китайская теорема об остатках и находится x.

Такой алгоритм может быть эффективным и реализован с полиномиальной сложностью $O\left(\left(\log_2 p\right)^2\right)$, если число $(p - 1)$ является гладким [7]. Из этого следует, что если факторизация $(p - 1)$ заранее не известна, то необходимость в факторизации не усложняет задачу. Однако следует иметь в виду, что в криптографии используются простые числа p достаточно большой разрядности, тогда возникает проблема в на-

хождении таких чисел таким образом, чтобы (p – 1) были разложены на небольшие простые множители. Может возникнуть ситуация, когда невозможно найти гладкое число, необходимое для решения конкретной задачи.

На данный момент алгоритмы нахождения гладких чисел неизвестны, что значительно усложняет использование приведенного выше алгоритма. До сих пор свойства гладких чисел и их распределение не исследовались. Однако в случае появления эффективных алгоритмов поиска простых чисел p, для которых (p – 1) является гладким, алгоритмы с открытым ключом могут стать непригодными для использования. Далее, в работе, такого типа простое число p будет называться гладким простым числом.

Будем называть простое число p *гладким простым числом*, для которого:

$$p = \prod_{i=1}^{k} p_i^{\alpha_i} + 1, \tag{2}$$

где p_i – простые числа, расположенные подряд в ряду простых чисел или с некоторым промежутком между ними. Разница между множителями влияет на сглаживание чисел. Решение проблемы построения меры гладкости является неисследованной областью в теории чисел и является темой для дальнейших исследований и анализа.

В зависимости от последовательности возрастания простых множителей гладкие числа можно классифицировать следующим образом:

Идеально гладкие простые числа - это такие числа, что для равенства (2) $p_i = 2,3,5, \ldots, p_k$. Это означает, что все простые множители являются последовательными простыми числами. Примеры таких чисел представлены в таблице 1.

Таблица 1 – Идеально гладкие простые числа

p	$\prod_{i=1}^{k} p_i^{\alpha_i}$
172161991	$2^4 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 13^2$
172972801	$2^8 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
174414241	$2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11^3 \cdot 13$
175134961	$2^4 \cdot 3^7 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
176576401	$2^4 \cdot 3^2 \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13$
177627451	$2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13^3$
174594421	$2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

Этот тип гладких чисел позволит найти дискретный логарифм в соответствии с алгоритмом [3] с полиномиальной сложностью [7]. Однако наряду с определением идеально гладкого числа возникает вопрос о количестве таких чисел. Может случиться так, что поиск гладкого числа большой размерности будет иметь высокую

алгоритмическую сложность, что, в свою очередь, делает использование алгоритма Сильвера-Полига-Хеллмана непрактичным.

Частично сглаженные простые числа. Предполагается, что для таких чисел последовательность простых множителей не обязательно является последовательными простыми числами, но разница между последовательными множителями не должна быть слишком большой. Пример частично сглаженных чисел показан в таблице 2.

Таблица 2 – Частично сглаженные простые числа

p	$\prod_{i=1}^{k} p_i^{\alpha_i}$
174485741	$2^2 \cdot 5 \cdot 11 \cdot 13^3 \cdot 19^2$
175468801	$2^8 \cdot 3 \cdot 5^2 \cdot 13 \cdot 19 \cdot 37$
170069761	$2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 19 \cdot 37$
170301751	$2 \cdot 3 \cdot 5^3 \cdot 17 \cdot 19^2 \cdot 37$

Частично гладкие простые числа также могут быть использованы для алгоритма [3], но его эффективность будет зависеть от меры гладкости таких чисел.

Открытой проблемой является эффективный поиск гладких чисел большой разрядности. Для этого необходимо знать, как распределяются простые числа в зависимости от количества множителей, поскольку при поиске дискретного логарифма нужно найти гладкие простые числа с достаточным количеством множителей. Это означает, что такие числа будут относиться к числу простых чисел, число множителей которых превышает определенное число.

На рисунке 1 показан график, изображающий последовательность простых множителей для идеально гладких простых чисел $p = 174594421$ (сплошная линия на графике) и частично гладких простых чисел $p = 170301751$ (пунктирная линия). По вертикальной оси нанесены простые множители p_i, по горизонтальной оси – значения i.

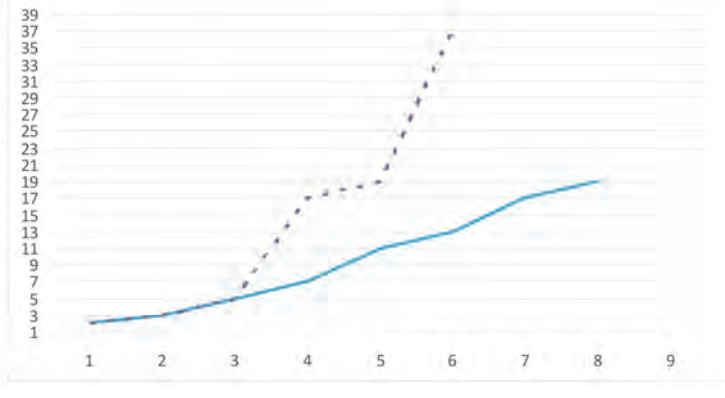

Рисунок 1 – Последовательность простых множителей для идеально гладких и частично гладких чисел.

В результате компьютерного моделирования, использованного для изучения свойств простых чисел, и решения гипотезы Артина в [8] были найдены простые множители для первых десяти миллионов простых чисел. Для такого объема количество простых множителей не превышает 8.

На рисунке 2 показан график распределения первых десяти миллионов простых чисел в зависимости от количества факторов. На горизонтальной оси нанесено количество простых множителей, а на вертикальной оси – количество соответствующих простых чисел.

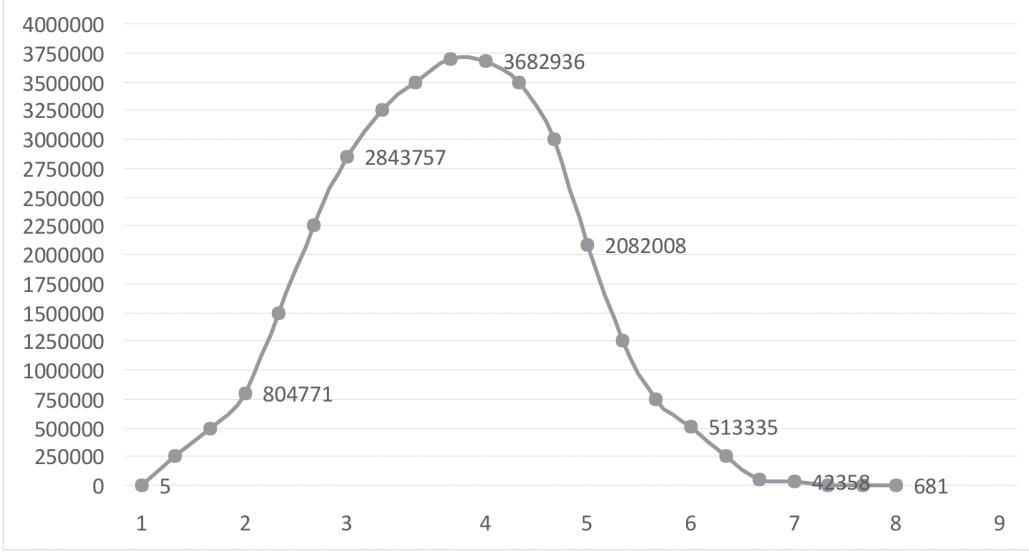

Рисунок 2 – Распределение первых десяти миллионов простых чисел в зависимости от количества множителей

Результаты и обсуждения. Исходя из полученных данных, можно предположить, что простые числа распределяются по одному из следующих законов:

1. Распределение χ^2 (хи-квадрат) с плотностью вероятности $f(x)=\frac{\left(1/2\right)^{\frac{k}{2}}}{\Gamma\left(k/2\right)}x^{\frac{k}{2}-1}e^{-\frac{x}{2}}$ где $\Gamma(x)=\int_0^{\infty}t^{x-1}e^{-t}dt$.

2. Распределение Стьюдента с плотностью $f(x)=\frac{\Gamma\left(k+1/2\right)}{\sqrt{n\pi}\Gamma\left(k/2\right)}\left(1+\frac{x^2}{k}\right)^{-\frac{k+1}{2}}$.

3. Логнормальное распределение с плотностью $f(x)=\frac{1}{x\sigma\sqrt{2\pi}}e^{-(\ln x-a)^2/2\sigma^2}$ с параметрами a и σ.

Открытым вопросом является проблема нахождения гладких простых чисел достаточной размерности и того, как они распределяются между простыми. Каждая из

задач, ранее перечисленных в работе, является фундаментальной проблемой современной математики и влияет на скорость реализации алгоритма Сильвера-Полига-Хеллмана и, соответственно, на возможность вычисления дискретного логарифма за полиномиальное время.

Заключение. Для решения задачи дискретного логарифмирования с использованием алгоритма Сильвера-Полига-Хеллмана важным моментом является использование гладких чисел, которые должны удовлетворять $(p-1) > 10^{300}$. Однако до сих пор неизвестно, как найти такие числа. Это затрудняет вычисление задачи. Для решения этой задачи необходимо решить ряд фундаментальных проблем теории чисел. Одной из них является определение закона распределения простых чисел, а также распределения гладких простых чисел среди простых чисел.

При анализе первых десяти миллионов простых чисел было обнаружено, что число идеально гладких чисел невелико и нет доказательств того, что их число бесконечно. Следовательно, в сокращенном алгоритме также необходимо учитывать частично гладкие простые числа.

Следующим важным фактором при решении задачи дискретного логарифмирования является мера гладкости простого числа, поскольку от этого напрямую зависит скорость выполнения алгоритма. Построение меры гладкости и анализ алгоритма в зависимости от гладкости числа - тема для дальнейшего изучения.

Благодарности. Работа выполнена при поддержке грантового финансирования по научно-техническим проектам Министерством науки и высшего образования Республики Казахстан, грант № AP19677733.

ЛИТЕРАТУРА

1 Smart N. Cryptography. – Moscow: Techno sphere, 2005.–528 p.

2 Манин Ю.И., Панчишкин А.А. Введение в современную теорию чисел. – Москва: МЦНМО, 2009. – 552 с.

3 Коблиц Н. Курс теории чисел и криптографии. – Москва: Научное изд–во ТВП, 2001. – 254 с.

4 Турусбекова, У., Муратбеков, М., Алтынбек, С., Ахатова, Ж. Исследование свойств структур рекурсивных циклов первообразных корней// Вестник КазНПУ им. Абая, Серия «Физико–математические науки». – 2023. –№3(83). DOI:https://doi.org/10.51889/2959–5894 .2023.83.3.007.

5 Ireland K., Rosen M. A Classical Introduction to Modern Number Theory. – New York: Springer, 1998.–394 p., ISBN 978-1-4757-2103-4.

6 Vostrov, G., Bezrukova Yu. Analysis and development of existing algorithms for solving the discrete logarithm problem // ELTECS ONPU, Астропринт. – 2018.– № 27, P. 242–247. – ISSN 2221–3805.

7 Pohlig S., Hellman M. An Improved Algorithm for Computing Logarithms Over GF(p) and its Cryptographic Significance //IEEE Transactions on Information Theory. – 1978. – №1 (24), P. 106-110.

8 Vostrov G., Opiata R. Generalized Artin hypothesis and computer information model its solutions // ELTECS ONPU, Астропринт. –2018.– №29, P. 120–126. – ISSN 2221-3805.

REFERENCES

1 Smart, N. (2005), Cryptography, – Moscow: Techno sphere, (p.528)

2 Manin, Yu., Panchishkin, A., (2009), Vvedeniye v sovremennuyu teoriyu chisel [Introduction to the modern theory of numbers] – Moscow: MCNMO, (p.552)

3 Koblitz, N. (2001), Kurs teorii chisel i kriptografii [Course of number theory and cryptography], Moscow: Scientific publishing house PTA, (p. 254)

4 Turusbekova, U., Muratbekov, M., Altynbek, S., Akhatova, Zh. (2023), Issledovaniye svoystv struktur rekursivnykh tsiklov pervoobraznykh korney[Research of the properties of the structures of recursive cycles of primitive roots] Vestnik KazNPU im. Abaya, Seriya «Fiziko–matematicheskiye nauki». – vol. 3(83). DOI:https://doi.org/10.51889/2959–5894.2023.83.3.007.

5 Ireland K., Rosen M. (1998), A Classical Introduction to Modern Number Theory. — New York: Springer, (p. 394), ISBN 978–1–4757–2103–4.

6 Vostrov, G., Bezrukova Yu. (2018), Analysis and development of existing algorithms for solving the discrete logarithm problem, ELTECS ONPU, Astroprint, 27, 242–247. – ISSN 2221–3805.

7 Pohlig, S, Hellman, M., (1978) An Improved Algorithm for Computing Logarithms Over GF(p) and its Cryptographic Significance – IEEE Transactions on Information Theory, vol. 1, no. 24, 106–110.

8 Vostrov, G. and Opiata, R. (2018), Generalized Artin hypothesis and computer information model its solutions, ELTECS ONPU, Astroprint, 29, 120–126. – ISSN 2221–3805.

У. К. ТУРУСБЕКОВА[1], М. Ә. БЕРСҰГІР[2]

[1]«Esil University» мекемесі, Астана, Қазақстан
[2]Абай атындағы Қазақ ұлттық педагогикалық университет, Алматы, Қазақстан

ДИСКРЕТТІ ЛОГАРИФМ ЕСЕПТЕРІНДЕГІ СИЛЬВЕР–ПОЛИГ–ХЕЛЛМАН АЛГОРИТМІН ЗЕРТТЕУ

Аталған жұмыста маңызды математикалық мәселе болып табылатын дискретті логарифм есебінің тұжырымы сипатталған. Сильвер–Полиг–Хеллманның дискретті логарифмдеуін есептеу алгоритмі талданған және оның кемшіліктері тегіс деп аталатын арнайы түрдегі сандарды қолданудан туындайды. Үлкен биттік тегіс жай сандарды іздеу кезінде пайда болатын мәселе көрсетілген. Мұндай сандарды іздеу процесі Сильвер–Полиг Хеллман алгоритмін баяулатады, сонымен қатар қажетті биттің тегіс жай сандарын табуға болатындығы белгісіз, өйткені жай сандар арасындағы олардың саны өте аз, бұл алгоритмді қолданудың тиімділігіне күмән келтіреді. Тегіс жай сан ұғымы енгізілді, қатарынан орналастырылған факторлардың өсуіне қарай мінсіз тегіс және жартылай тегіс жай сандарға жіктеу ұсынылды. Тегістікке алғашқы он миллион жай сандар талданды, олардың арасында өте тегіс бірнеше ондаған табылды. Тегіс жай сандарды табу және олардың қасиеттерін талдау үшін жай көбейткіштердің санына байланысты жай сандардың қалай бөлінетінін білу қажет екендігі көрсетілген. Алғашқы он миллион жай сандардың таралу нәтижелері келтірілген және ықтимал таралу заңдары туралы болжамдар берілген. Көршілес көбейткіштердің айырмашылығына және олардың дәрежесіне байланысты қарастырылуы керек тегістік өлшемін құру мәселесі келтірілген.

Түйін сөздер: *дискретті логарифм, жай сан, тегіс жай сан, алғашқы түбір, факторизация.*

U. K. TURUSBEKOVA[1], M. A. BERSUGIR[2]

[1]Institution "Esil University", Astana, Kazakhstan
[2]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan

INVESTIGATION OF THE SILVER–POHLIG–HELLMAN ALGORITHM IN DISCRETE LOGARITHM TASKS

This paper describes the formulation of the discrete logarithm problem, which is an important mathematical problem. The algorithm for calculating the Silver–Pohlig–Hellman discrete logarithm is analyzed and its disadvantages arising from the use of numbers of a special type called smooth are indicated. The problem that arises when searching for smooth primes of high bit depth is indicated. The process of searching for such numbers slows down the Silver–Pohlig Hellman algorithm, in addition, it is not known whether it is possible to find smooth primes of the required bit depth, because their number among the primes is extremely small, which calls into question the effectiveness of the algorithm. The concept of a smooth prime number is introduced, and a classification is proposed depending on the growth of consecutive multipliers into perfectly smooth and partially smooth primes. The first ten million primes were analyzed for smoothness, among which several tens were found to be perfectly smooth. It is shown that in order to search for smooth primes and analyze their properties, it is necessary to know how the primes are distributed depending on the number of prime factors. The results of the distribution of the first ten million primes are presented and assumptions about possible distribution laws are made. The problem of constructing a measure of smoothness is presented, which should be considered depending on the difference of adjacent factors and their degrees.

Key words: *discrete logarithm, prime number, smooth prime number, primitive root, factorization.*