UDC 681.3.06.

ANALYSIS OF SMOOTH NUMBERS SEARCH METHODS FOR SOLVING THE DISCRETE LOGARITHM PROBLEM

G. Vostrov, O. Ponomarenko
Odessa national polytechnic university

Abstract. *This paper describes the formulation of the discrete logarithm problem, which is an important mathematical problem. The algorithm for computing the discrete logarithm of Silver-Pohlig-Hellman is analyzed and its drawbacks arising from the use of numbers of a special type, called smooth, are indicated. The concept of a smooth prime number was introduced, a classification was introduced depending on the increase of the successive factors on the perfectly smooth and partially smooth prime numbers. It is shown that to search for smooth primes and analyze their properties, it is necessary to know how primes are distributed depending on the number of simple factors. The problem of constructing a measure of smoothness is given.*

Key words: *discrete logarithm, prime number, smooth prime number, primitive root, chi-squared distribution, Student's t-distribution, lognormal distribution, cryptography.*

Introduction

The problem of discrete logarithm is one of the fundamental mathematical problems. At the moment there are no efficient algorithms for computing the discrete logarithm. This became the basis for creating cryptographic public-key algorithms in the early 80s, which are widely used to this day.

The basic idea of public-key algorithms is to find some easily accomplished at the stage of encrypting a mathematical transformation that would be difficult to reverse without knowledge of secret information. Such a transformation is one-way functions [1]. These functions include the function of discrete exponentiation, and for its inversion it is required to calculate the discrete logarithm.

For multiplicative groups of a finite field and for groups similar to elliptic curves, there are no effective polynomial computation algorithms. Most of the methods have an exponential or subexponential complexity. However, in the case of the implementation of efficient algorithms for computing the discrete logarithm, all cryptographic systems based on it will become unsuitable. Until now, the existence of such an algorithm is an open question.

In [2], [3], a fast algorithm is considered, in which certain type of numbers, called "smooth", are used. This algorithm promises a polynomial complexity, in the case when deductions are modulo a simple smooth number, therefore, the question arises about the effective finding of such numbers, and the distribution of these numbers among prime numbers, since in applied aspects of cryptography these are numbers of high capacity. However, there is no clear definition of the concept of smoothness. Another problem is the search for numbers of this type. Further, the paper will consider the algorithm proposed by Silver, Pohlig and Hellman, and also propose a classification of smooth numbers and present their distribution.

1. Silver-Pohlig-Hellman Discrete Logarithm Algorithm

The discrete logarithm problem is considered in a residue ring modulo a prime number $(Z/mZ)^*$. The task is to find $x, 0 \le x < p-1$, satisfying the following comparison:

$$a = b^x \pmod p \qquad (1),$$

Where a, b, p are known, and $(p-1)$ is smooth (all its divisors are small) and all its decompositions q_i into simple dividers $p-1=\prod_{i=1}^{k} q_i^{\alpha_i}$ are known [5]. At the same time, Koblits assumes that b it is a primitive root modulo p [3]. This means that together with its class of residues it generates a group $(Z/pZ)^*$ [4]. However, it should be borne in mind that with such a formulation, the algorithm is only a special case of the discrete logarithm solution. Also, its use requires the existence of algorithms for finding smooth numbers.

The algorithm from [3] contains the following steps:

1. For each simple divisor q, the values $r_{q_i,j} = b^{\frac{j(p-1)}{q_i}}$ are calculated, where $j=\overline{0,(q_i-1)}$. For the construction b of a greater degree, the method of successive squaring is used [2].

2. It is assumed that $x \equiv x_0 + x_1 q_i + \ldots + x_{\alpha_i - 1} q_i^{\alpha_i - 1} \pmod p$, where

$x_i = \overline{0, q_i - 1}$. To find x_0, it is calculated $a^{\frac{p-1}{q_i}} = b^{\frac{x(p-1)}{q_i}} = b^{\frac{x_0(q-1)}{p}} = r_{q_i, x_0}$. Then $x_0 = j$, if $a^{\frac{p-1}{q_i}} = r_{q_i, j}$.

3. $a_k^{\frac{p-1}{q_i^{k+1}}} = b^{\frac{(x_k + x_{k+1} q_i)(p-1)}{q_i}} = b^{\frac{x_k (p-1)}{q_i}} = r_{q_i, x_k}$

for each $k = \overline{1, \alpha_i - 1}$, we find $x_k = j$, if $a_k^{\frac{p-1}{q_i^{k+1}}} = r_{q_i, j}$.

4. Upon completion, the Chinese theorem on residuals is used and is found x.

Such an algorithm can be efficient and implemented with polynomial complexity $O((\log_2 p)^2)$ if the number $(p-1)$ is smooth [6]. From this it follows that if the factorization $(p-1)$ is not known in advance, the need for factorization does not complicate the task. However, it should be borne in mind that in cryptography are used simple numbers p of sufficiently large digit capacity, then there is a problem in finding such numbers so that $(p-1)$ they are decomposed into small simple factors. A situation may arise when it is impossible to find a smooth number required to solve a specific problem.

At the moment, algorithms for finding smooth numbers are not known, which greatly complicates the use of the above algorithm. Until now, the properties of smooth numbers and their distribution have not been investigated. However, in the case of the emergence of effective algorithms for the search for primes p, for which $(p-1)$ is smooth, public-key algorithms may become unsuitable for use. Further, in a work of this type, a prime number p will be called a smooth prime number.

2. The definition of the concept of smoothness of numbers and their classification

We will call such a prime number p smooth prime number, for which:

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

where p_i are the prime numbers that are arranged in a row in the row of prime numbers or with some gap between them. The difference between the factors affects the smoothness of the numbers. The solution to the problem of constructing a measure of smoothness is an unexplored area in the theory of numbers and is a topic for further research and analysis.

Depending on the sequence of increasing simple factors, smooth numbers can be classified as follows:

1. Perfectly smooth prime numbers are numbers such that for (2), $p_i = 2,3,5,..., p_k$. This means that all prime factors are consecutive prime numbers. Examples of such numbers are presented in Table 1.

Table 1

Perfectly smooth primes

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	$2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

This type of smooth numbers will allow finding the discrete logarithm according to the algorithm [3] with polynomial complexity [6]. However, along with the definition of a perfectly smooth number, the question arises as to the number of such numbers. It may happen that the search for a smooth number of large dimension will have a high algorithmic complexity, which in turn makes the use of the Silver-Pohlig-Hellman algorithm impractical.

2. Partially smooth prime numbers. It is assumed that for such numbers the sequence of prime factors is not necessarily consecutive prime numbers, but the difference between consecutive multipliers should not be too large. An example of partially smooth numbers is shown in Table 2.

Table 2

Partially smooth primes

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	$2 \cdot 3 \cdot 5^3 \cdot 17 \cdot 19^2 \cdot 37$

Partially smooth primes can also be used for the algorithm [3], but its efficiency will depend on the measure of the smoothness of such numbers.

An open problem is the effective search for smooth numbers of large bitness. To do this, you need to know how primes are distributed depending on the number of factors, since when finding a dis-

crete logarithm, you need to find smooth primes with a sufficient number of factors. This means that such numbers will be among the prime numbers, the number of factors that have more than a certain number.

Fig. 1 shows a graph depicting a sequence of simple factors for perfectly smooth $p = 174594421$ (solid line on the graph) and partially smooth $p = 170301751$ (dashed line) prime numbers. On the vertical axis, prime multipliers p_i are plotted, on the horizontal axis – i values.

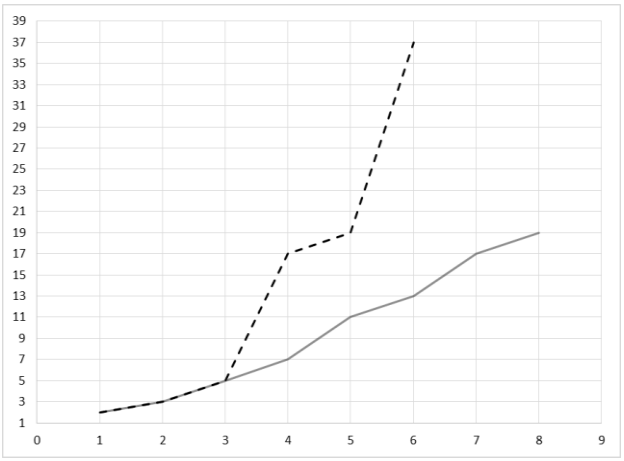

Fig. 1 A sequence of prime factors for perfectly smooth and partially smooth numbers.

As a result of computer simulation used to study the properties of primes and the solution of the Artin hypothesis in [7], simple factors for the first 10 million primes were found. For such a volume, the number of simple factors does not exceed 8.

Fig. 2 shows a graph of the distribution of the first 10 million primes depending on the number of factors. The number of simple factors on the horizontal axis is plotted, and the number of corresponding primes on the vertical axis.

Based on the data obtained, it can be assumed that prime numbers are distributed according to one of the following laws:

1. Chi-squared distribution χ^2 with probability density $f(x) = \frac{\left(1/2\right)^{\frac{k}{2}}}{\Gamma\left(k/2\right)} x^{\frac{k}{2}-1} e^{-\frac{x}{2}}$, where $\Gamma(x) = \int_0^{\infty} t^{x-1} e^{-t} dt$.

2. Student's distribution with density $f(x) = \frac{\Gamma(k+1/2)}{\sqrt{n\pi}\Gamma(k/2)} \left(1 + \frac{x^2}{k}\right)^{-\frac{k+1}{2}}$.

3. Lognormal distribution with density $f(x) = \frac{1}{x\sigma\sqrt{2\pi}} e^{-(\ln x - a)^2 / 2\sigma^2}$ with parameters a and σ.

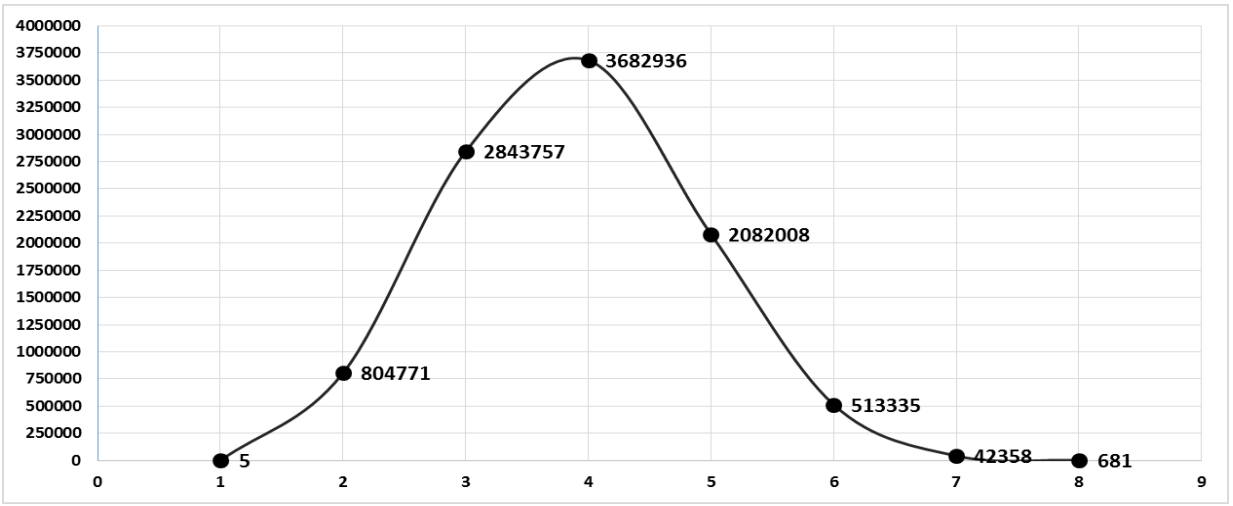

Fig 2. The distribution of the first 10 million primes depending on the number of factors

An open question is the problem of finding smooth primes of sufficient dimension and how they are distributed among the simple ones. Each of the problems previously listed in the paper is a fundamental problem of modern mathematics and affects the speed of the implementation of the Silver-Pohlig-Hellman algorithm and, accordingly, the possibility of calculating the discrete logarithm for polynomial time.

Conclusions

To solve the discrete logarithm problem using the Silver-Pohlig-Hellman algorithm, an important point is the use of smooth numbers which must satisfy $(p-1) > 10^{300}$. However, it is still not known how to find such numbers. This makes the task diffi-

cult to compute. To solve this problem, a number of fundamental problems of the theory of numbers must be solved. One of them is the definition of the law of distribution of primes, as well as the distribution of smooth prime numbers among primes.

When analyzing the first 10 million prime numbers, it was found that the number of perfectly smooth numbers is small and there is no evidence that their number is infinite. Therefore, it is also necessary to consider partially smooth prime numbers in the reduced algorithm.

The next important factor in solving the problem of discrete logarithm is a measure of the smoothness of a prime number, since the execution rate of the algorithm directly depends on this. The construction of the smoothness measure and the analysis of the algorithm depending on the smoothness of the number is a topic for further study.

References

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

2. Manin, Yu., Panchishkin, A., (2009), Introduction to the modern theory of numbers - Moscow: MSC-MO, 552 p.

3. Koblitz, N. (2001), Course of number theory and cryptography, Moscow: Scientific publishing house PTA, 254 p.

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

5. Vostrov, G., Bezrukova Yu. (2018), "Analysis and development of existing algorithms for solving the discrete logarithm problem", ELTECS ONPU, Астропринт, vol. 27, pp. 242-247. – ISSN 2221-3805.

6. 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. pp. 106-110.

7. Vostrov, G. and Opiata, R. (2018), "Generalized Artina hypothesis and computer information model its solutions", ELTECS ONPU, Астропринт, vol. 29, pp. 120-126. – ISSN 2221-3805.

АНАЛІЗ МЕТОДІВ ПОШУКУ ГЛАДКИХ ЧИСЕЛ ДЛЯ ВИРІШЕННЯ ЗАДАЧІ ДИСКРЕТНОГО ЛОГАРИФМУВАННЯ

Востров Г. М., Пономаренко О. Ю.
Одеський національний політехнічний університет

Анотація. *У даній роботі описана постановка задачі дискретного логарифмування, яка є важливою математичної проблемою, яка наразі є невирішеною. Проаналізовано алгоритм обчислення дискретного логарифма Силвера-Поліга-Хеллмана і вказані його недоліки, що виникають через використання чисел спеціального типу, званих гладкими. Вказана проблема, яка виникає при пошуку гладких простих чисел великої розрядності. Процес пошуку таких чисел уповільнює алгоритм Силвера-Поліга-Хеллмана, крім того не відомо чи можливо знайти гладкі прості числа необхідної розрядності, адже їх кількість серед простих чисел надзвичайно мала, що ставить під питання ефективність використання алгоритму. Було введено поняття гладкого простого числа, запропонована класифікація в залежності від зростання поспіль розташованих множників на ідеально гладкі і частково гладкі прості числа. Були проаналізовані перші десять мільйонів простих чисел на гладкість, серед яких ідеально гладких виявлено кілька десятків. Виникає необхідність у перевірці гіпотези про кінцеву кількість ідеально гладких чисел. Частково гладкі прості числа можуть значно уповільнити роботу алгоритму, адже невідома точна структура числа, кількість співмножників та різниця між ними. Також враховується, що при зростанні простих чисел, різниця між ними теж зростатиме. Показано, що для пошуку гладких простих чисел і аналізу їх властивостей необхідно знати, як розподілені прості числа в залежності від кількості простих співмножників, адже у випадку задачі дискретного логарифмування необхідно знаходити гладкі числа з кількістю співмножників більшою за 5-6. Наведені результати розподілу перших десяти мільйонів простих чисел та видвинуті припущення щодо можливих законів розподілу. Наведено проблема побудови міри гладкості, яка має бути розглянута в залежності від різниці суміжних співмножників та їх степенів.*

Ключові слова: *дискретний логарифм, просте число, гладке просте число, первісний корінь, розподіл хі-квадрат, розподіл Стьюдента, логнормальний розподіл, криптографія.*

АНАЛИЗ МЕТОДОВ ПОИСКА ГЛАДКИХ ЧИСЕЛ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

Востров Г. Н., Пономаренко Е. Ю.
Одесский национальный политехнический университет

Аннотация. *В данной работе описана постановка задачи дискретного логарифмирования, которая является важной математической проблемой. Проанализирован алгоритм вычисления дискретного логарифма Силвера-Полига-Хеллмана и указаны его недостатки, возникающие из-за использования чисел специального типа, называемых гладкими. Было введено понятие гладкого простого числа, предложена классификация в зависимости от роста подряд расположенных множителей на идеально гладкие и частично гладкие простые числа.*

Ключевые слова: *дискретный логарифм, простое число, гладкое простое число, первообразный корень, распределение хи-квадрат, распределение Стьюдента, логнормальное распределение, криптография.*

Received 08.04.2019

George Vostrov, Ph. D. of Technical Sciences, Associate Professor of the Department of Applied Mathematics and Information Technologies, Odessa National Polytechnic University. Shevchenko ave., 1, Odessa, Ukraine.
E-mail: vostrov@gmail.com, mob. +380503168776

Востров Георгій Миколайович, кандидат технічних наук, доцент кафедри прикладної математики та інформаційних технологій Одеського національного політехнічного університету. Проспект Шевченко, 1, Одеса, Україна.
E-mail: vostrov@gmail.com, тел. +380503168776

ORCID ID: 0000-0003-3856-5392

Olena Ponomarenko, Student of the Department of Applied Mathematics and Information Technologies, Odessa National Polytechnic University. Shevchenko ave., 1, Odessa, Ukraine.
E-mail: ponomarenkoelena1997@gmail.com, mob. +380934321669

Пономаренко Олена Юріївна, студент кафедри прикладної математики та інформаційних технологій, Одеського національного політехнічного університету. Проспект Шевченко, 1, Одеса, Україна.
E-mail: ponomarenkoelena1997@gmail.com, тел. +380934321669

ORCID ID: 0000-0003-1585-4706