А.О.Гельфонд и теоретико - числовые исследования в криптографии

Ю.В. Нестеренко
Механико-математический факультет
МГУ имени М.В. Ломоносова

22.04.2025

Александр Осипович ГЕЛЬФОНД

Родился 24(11) октября 1906 г. в семье врача в Петербурге, умер 7 ноября 1968 г. в Москве. Поступил в Московский университет в 1924 г. и окончил его в 1927 г., аспирантуру окончил в 1930 г., с 1931 г. профессор МГУ, с 1933 г. работал также в Математическом институте им. В. А. Стеклова.

Александр Осипович ГЕЛЬФОНД

Родился 24(11) октября 1906 г. в семье врача в Петербурге, умер 7 ноября 1968 г. в Москве. Поступил в Московский университет в 1924 г. и окончил его в 1927 г., аспирантуру окончил в 1930 г., с 1931 г. профессор МГУ, с 1933 г. работал также в Математическом институте им. В. А. Стеклова.

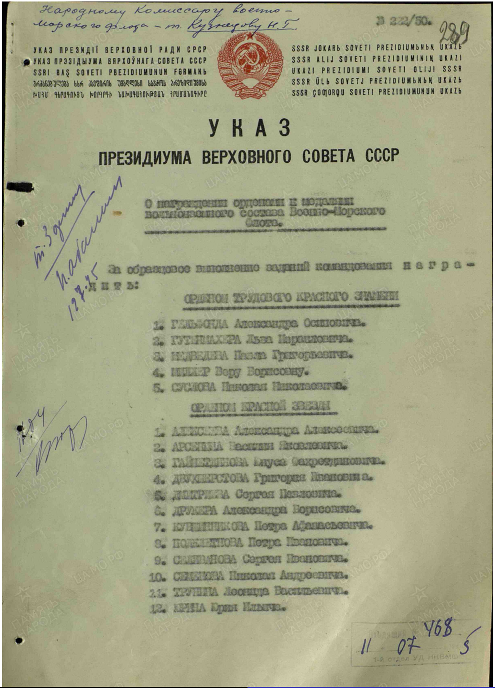
Ученая степень доктора физико-математических наук была присвоена Александру Осиповичу в 1935 г., в 1939 г. он избран членом - корреспондентом АН СССР. С 1968 г.— член-корреспондент Международной академии истории науки в Париже.

Александр Осипович ГЕЛЬФОНД

Родился 24(11) октября 1906 г. в семье врача в Петербурге, умер 7 ноября 1968 г. в Москве. Поступил в Московский университет в 1924 г. и окончил его в 1927 г., аспирантуру окончил в 1930 г., с 1931 г. профессор МГУ, с 1933 г. работал также в Математическом институте им. В. А. Стеклова.

Ученая степень доктора физико-математических наук была присвоена Александру Осиповичу в 1935 г., в 1939 г. он избран членом - корреспондентом АН СССР. С 1968 г.— член-корреспондент Международной академии истории науки в Париже.

Александр Осипович был награжден орденом Ленина (1953), тремя орденами Трудового Красного Знамени (11.06.1945; 8.07.1945; 1966) и медалями.



Народному Комиссару военно-морского флота – т. Кузнецову Н.Г.

В 222/50.

289

УКАЗ ПРЕЗИДІЇ ВЕРХОВНОЇ РАДИ СРСР
УКАЗ ПРЭЗІДЫУМА ВЯРХОЎНАГА СОВЕТА СССР
SSRI BAŞ SOVETI PREZIDIUMUNUN FƏRMANЬ
SSSR JOKARЬ SOVETI PREZIDIUMЬNЬŊ UKAZЬ
SSSR ALIJ SOVETI PREZIDIUMINIŊ UKAZI
UKAZI PREZIDIUMI SOVETI OLIJI SSSR
SSSR ÜLЬ SOVETJ PREZIDIUMЬNЬŊ UKAZЬ
SSSR ÇOQORQU SOVETI PREZIDIUMUNUN UKAZЬ

У К А З
ПРЕЗИДИУМА ВЕРХОВНОГО СОВЕТА СССР

О награждении орденами и медалями вольнонаемного состава Военно-Морского Флота.

За образцовое выполнение заданий командования н а г р а д и т ь:

ОРДЕНОМ ТРУДОВОГО КРАСНОГО ЗНАМЕНИ

1. ГЕЛЬФОНДА Александра Осиповича.
2. ГУТЕНМАХЕРА Льва Израилевича.
3. МЕДВЕДЕВА Павла Григорьевича.
4. [illegible] Веру Борисовну.
5. СУСЛОВА Николая Николаевича.

ОРДЕНОМ КРАСНОЙ ЗВЕЗДЫ

1. [illegible] Александра Алексеевича.
2. АРСЕНИНА Василия Яковлевича.
3. [illegible] [illegible] [illegible].
4. ДВУХШЕРСТОВА Григория Ивановича.
5. ДМИТРИЕВА Сергея Павловича.
6. ДРУКЕРА Александра Борисовича.
7. КУВШИННИКОВА Петра Афанасьевича.
8. [illegible] Петра Ивановича.
9. СЕЛИВАНОВА Сергея Ивановича.
10. СЕМЕНОВА Николая Андреевича.
11. ТРУНИНА Леонида Васильевича.
12. ЮРИНА Юрия Ильича.

Входящий № 468
11 07 5
1-й отдел УД НКВМФ

292

69. ЧУГУНОВУ Софью Павловну.
70. ЛИЦКОГО Николая Пантелеймоновича.
71. ПРЯКОВУ Марию Васильевну.
72. ЯКОВЛЕВУ Елену Дмитриевну.

Председатель Президиума
Верховного Совета СССР – М.КАЛИНИН.

Секретарь Президиума
Верховного Совета СССР – А. Горкин
(А.Горкин)

Москва, Кремль.
8 июля 1945 г.
д.№ 255/473.

НАГРАДНОЙ ЛИСТ

235

на старшего научного сотрудника 11 Отдела Ру ГМ ВМФ
(должность, наименование войсковой части, соединения, учреждения или заведения)

ГЕЛЬФОНД Александра Осиповича
(военное звание, фамилия, имя и отчество)

"ТРУДОВОЕ КРАСНОЕ ЗНАМЯ"
(наименование награды)

1. Год рождения 1906 г.
2. Национальность Еврей
3. Соцположение Служащий
4. Партийность чл.ВКП(б) с 1940 г.
5. С какого времени в РККА и ВМФ Вольнонаемный
6. Участие в гражданской войне Не участвовал
7. Ранения и контузии Не имеет
8. Представлялся ли ранее к награде, когда и за что Не представлялся
9. Какие имеет поощрения и награды и за что Не имеет
10. Служба в белой или других буржуазных армиях, пребывание в плену и в окружении Не был
11. Постоянный адрес:

ДЛЯ ПОДШИВКИ

I. Краткое, конкретное изложение личного боевого подвига или заслуг
(составляется в штабе войсковой части, соединения, учреждения или заведения)

Член корреспондент Академии Наук СССР, доктор

НАГРАДНОЙ ЛИСТ

на старшего научного сотрудника 11 Отдела РУ ГМШ ВМФ
ГЕЛЬФОНД Александра Осиповича
«ТРУДОВОЕ КРАСНОЕ ЗНАМЯ» (наименование награды)

1. **Год рождения** 1906 г.
2. **Национальность** Еврей
3. **Соцположение** Служащий
4. **Партийность** чл.ВКП(б) с 1940 г.
5. **С какого времени в РККА и ВМФ** Вольнонаёмный
6. **Участие в гражданской войне** Не участвовал
7. **Ранения и контузии** Не имеет
8. **Представлялся ли ранее к награде, когда и за что** Не представлялся
9. **Какие имеет поощрения и награды и за что** Не имеет
10. **Служба в белой или других буржуазных армиях, пребывание в плену и в окружении** Не был
11. **Постоянный адрес**

Продолжение Наградного листа

Краткое, конкретное изложение личного боевого подвига или заслуг (составляется в штабе войсковой части, соединения учреждения или заведения)

Член корреспондент Академии наук СССР, доктор математических наук, профессор тов. Гельфонд пришёл в разведку в период Отечественной войны с тем, чтобы все свои знания и опыт выдающегося учёного отдать непосредственно делу разгрома гитлеровской Германии.

Будучи научным руководителем научно-исследовательского Отделения тов. Гельфонд лично разрешил ряд сложнейших теоретических проблем, имевших большое практическое значение.

С 1931 г. А.О. Гельфонд работал на физ.-мех., а после реорганизации в апреле 1933 года — на мех.-мат. факультете МГУ. В 1938 году кафедра анализа и теории функций была разделена на кафедру теории функций и кафедру математического анализа, заведующим которой стал А. О. Гельфонд, возглавлявший её до 1943 года. С 1948 года до конца своей жизни Гельфонд был заведующим кафедрой теории чисел и одновременно кабинета истории математики. Александр Осипович был выдающимся педагогом. Среди его учеников — более 10 докторов наук и 30 кандидатов наук.

С 1931 г. А.О. Гельфонд работал на физ.-мех., а после реорганизации в апреле 1933 года — на мех.-мат. факультете МГУ. В 1938 году кафедра анализа и теории функций была разделена на кафедру теории функций и кафедру математического анализа, заведующим которой стал А. О. Гельфонд, возглавлявший её до 1943 года. С 1948 года до конца своей жизни Гельфонд был заведующим кафедрой теории чисел и одновременно кабинета истории математики. Александр Осипович был выдающимся педагогом. Среди его учеников — более 10 докторов наук и 30 кандидатов наук.

Во время Великой Отечественной войны Гельфонд был привлечён к работам в области криптографии при Главном Штабе Военно-Морского Флота.

С 1931 г. А.О. Гельфонд работал на физ.-мех., а после реорганизации в апреле 1933 года — на мех.-мат. факультете МГУ. В 1938 году кафедра анализа и теории функций была разделена на кафедру теории функций и кафедру математического анализа, заведующим которой стал А. О. Гельфонд, возглавлявший её до 1943 года. С 1948 года до конца своей жизни Гельфонд был заведующим кафедрой теории чисел и одновременно кабинета истории математики. Александр Осипович был выдающимся педагогом. Среди его учеников — более 10 докторов наук и 30 кандидатов наук.

Во время Великой Отечественной войны Гельфонд был привлечён к работам в области криптографии при Главном Штабе Военно-Морского Флота.

С 1933 г. до конца жизни А. О. Гельфонд работал в ФМИ, в дальнейшем — в МИАН (работать в МИАН начал еще в период пребывания Института до 1934 г. в Ленинграде) — старший научный сотрудник в 1933–1939 гг. и в 1944–1960 гг., заведующий Отделом теории чисел в 1939–1941 гг., заведующий Отделом теории функций в 1942–1943 гг., заведующий лабораторией № 1 Отдела прикладных расчетов в 1960–1968 гг.

Из интервью В.И. Арнольда, 2007 г.

Верно ли мнение, что подразделения криптографии КГБ были школой подготовки математических гениев и внесли свой вклад в науку?

Из интервью В.И. Арнольда, 2007 г.

Верно ли мнение, что подразделения криптографии КГБ были школой подготовки математических гениев и внесли свой вклад в науку?— На мой взгляд, никакой пользы для математики в России от криптографии не было, так же, как от бухгалтерии и других применений таблицы умножения, разве что зарплата участвовавшим математикам. Верно, однако, что для криптографии польза от математических гениев была огромная.

Из интервью В.И. Арнольда, 2007 г.

Верно ли мнение, что подразделения криптографии КГБ были школой подготовки математических гениев и внесли свой вклад в науку?— На мой взгляд, никакой пользы для математики в России от криптографии не было, так же, как от бухгалтерии и других применений таблицы умножения, разве что зарплата участвовавшим математикам. Верно, однако, что для криптографии польза от математических гениев была огромная. Например, один из лучших математиков России— — Александр Осипович Гельфонд (24 ноября 2006 года мы отпраздновали 100-летие со дня его рождения)— был главным криптографом флота во время войны. По-моему, с генеральским чином в соответствующем комитете. Он знаменит не только своими гениальными работами по теории чисел (за которые, однако, его так и не выбрали почему-то в академики, хотя член-корреспондентом он был выбран в молодости), но и своими секретными работами. Мало кто в мире подозревал, что Александр Осипович— не академик.

А.П. Юшкевич, профессор, историк математики об А.О. Гельфонде

Гельфонд — занимался теорией чисел и теми вопросами теории аналитических функций, которые к ней примыкают. Я знаком был с Гельфондом еще до того, как поступил в университет. Наши отцы были знакомы, и мы познакомились таким вот образом. Необыкновенной силы был математик. Необыкновенной, среди математиков, силы был шахматист, великолепно играл в шахматы и университет представлял на первой доске в свое время. Очень, очень сильной вообще мысли человек, очень волевая натура.

А.П. Юшкевич, профессор, историк математики об А.О. Гельфонде

Гельфонд — занимался теорией чисел и теми вопросами теории аналитических функций, которые к ней примыкают. Я знаком был с Гельфондом еще до того, как поступил в университет. Наши отцы были знакомы, и мы познакомились таким вот образом. Необыкновенной силы был математик. Необыкновенной, среди математиков, силы был шахматист, великолепно играл в шахматы и университет представлял на первой доске в свое время. Очень, очень сильной вообще мысли человек, очень волевая натура. Есть математики, которые не интересуются историей своей науки и даже считают, что это ненужное дело. Есть другие, которым кажется это и полезным, и интересным. Гельфонд принадлежал ко второй категории, его история математики интересовала.

А.П. Юшкевич, профессор, историк математики об А.О. Гельфонде

Гельфонд — занимался теорией чисел и теми вопросами теории аналитических функций, которые к ней примыкают. Я знаком был с Гельфондом еще до того, как поступил в университет. Наши отцы были знакомы, и мы познакомились таким вот образом. Необыкновенной силы был математик. Необыкновенной, среди математиков, силы был шахматист, великолепно играл в шахматы и университет представлял на первой доске в свое время. Очень, очень сильной вообще мысли человек, очень волевая натура. Есть математики, которые не интересуются историей своей науки и даже считают, что это ненужное дело. Есть другие, которым кажется это и полезным, и интересным. Гельфонд принадлежал ко второй категории, его история математики интересовала.Гельфонд был человеком огромного ума, огромной культуры, в высшей степени обаятельный в обращении.

В 1900 году крупнейший математик того времени Давид Гильберт на математическом конгрессе в Париже выдвинул список нерешенных проблем, которые он считал наиболее перспективными и важными для будущего математики. Среди них была седьмая проблема — касающаяся трансцендентных чисел. В 29-м г. Гельфонд получил первые свои результаты в теории трансцендентных чисел, а потом и полное решение седьмой проблемы. Эти работы прославили его на весь мир.

В 1900 году крупнейший математик того времени Давид Гильберт на математическом конгрессе в Париже выдвинул список нерешенных проблем, которые он считал наиболее перспективными и важными для будущего математики. Среди них была седьмая проблема — касающаяся трансцендентных чисел. В 29-м г. Гельфонд получил первые свои результаты в теории трансцендентных чисел, а потом и полное решение седьмой проблемы. Эти работы прославили его на весь мир. Через некоторое время он был командирован на несколько месяцев в Германию, по-моему в Геттинген, где как раз и жил этот знаменитый Гильберт, уже к тому времени пожилой человек. Вскоре Гельфонд выдвинулся в ряды первых специалистов по теории чисел и, весьма молодым был выбран членом-корреспондентом Академии наук.

В 1900 году крупнейший математик того времени Давид Гильберт на математическом конгрессе в Париже выдвинул список нерешенных проблем, которые он считал наиболее перспективными и важными для будущего математики. Среди них была седьмая проблема — касающаяся трансцендентных чисел. В 29-м г. Гельфонд получил первые свои результаты в теории трансцендентных чисел, а потом и полное решение седьмой проблемы. Эти работы прославили его на весь мир. Через некоторое время он был командирован на несколько месяцев в Германию, по-моему в Геттинген, где как раз и жил этот знаменитый Гильберт, уже к тому времени пожилой человек. Вскоре Гельфонд выдвинулся в ряды первых специалистов по теории чисел и, весьма молодым был выбран членом-корреспондентом Академии наук.

Когда в 1957 году на торжественной сессии Академии наук в Ленинграде отмечалось 250-летие со дня рождения Эйлера, Гельфонд сделал великолепный доклад о работах по теории чисел этого Эйлера. Доклад был потом напечатан и стал одной из лучших, я думаю, работ об Эйлере, которые выходили за многие и многие годы, по глубине проникновения в существо творчества Эйлера.

Алгебраические и трансцендентные числа

Число называется **алгебраическим**, *если оно есть корень многочлена с рациональными коэффициентами. В противном случае оно называется* **трансцендентным.**

Алгебраические и трансцендентные числа

Число называется **алгебраическим**, *если оно есть корень многочлена с рациональными коэффициентами. В противном случае оно называется* **трансцендентным.**

Трансцендентные числа: e (Эрмит, 1873), π (Линдеман, 1882).

Алгебраические и трансцендентные числа

Число называется **алгебраическим**, *если оно есть корень многочлена с рациональными коэффициентами. В противном случае оно называется* **трансцендентным.**

Трансцендентные числа: e (Эрмит, 1873), π (Линдеман, 1882).

7-я проблема Гильберта (две эквивалентные формулировки:)

1. Степень a^b при алгебраическом основании a и алгебраическом иррациональном показателе b есть трансцендентное число.

$2^{\sqrt{2}}, \quad e^{\pi} = i^{-2i}$

2. Если α и β - алгебраические числа, отношение $\frac{\ln \beta}{\ln \alpha}$ определено и иррационально, то это отношение трансцендентно.

$\frac{\ln 3}{\ln 2}, \quad \frac{\ln 4}{\ln_2} = 2.$

Алгебраические и трансцендентные числа

Число называется **алгебраическим**, *если оно есть корень многочлена с рациональными коэффициентами. В противном случае оно называется* **трансцендентным.**

Трансцендентные числа: e (Эрмит, 1873), π (Линдеман, 1882).

7-я проблема Гильберта (две эквивалентные формулировки:)

1. Степень a^b при алгебраическом основании a и алгебраическом иррациональном показателе b есть трансцендентное число.

$2^{\sqrt{2}}, \quad e^{\pi} = i^{-2i}$

2. Если α и β - алгебраические числа, отношение $\frac{\ln \beta}{\ln \alpha}$ определено и иррационально, то это отношение трансцендентно.

$\frac{\ln 3}{\ln 2}, \quad \frac{\ln 4}{\ln_2} = 2.$

Эйлер (гипотеза): *Логарифм алгебраического числа по алгебраическому основанию может быть либо рациональным числом, либо числом трансцендентным.* $\log_2 3 = \frac{\ln 3}{\ln 2}$.

Алгебраические и трансцендентные числа

Число называется **алгебраическим**, *если оно есть корень многочлена с рациональными коэффициентами. В противном случае оно называется* **трансцендентным.**

Трансцендентные числа: e (Эрмит, 1873), π (Линдеман, 1882).

7-я проблема Гильберта (две эквивалентные формулировки:)

1. Степень a^b при алгебраическом основании a и алгебраическом иррациональном показателе b есть трансцендентное число.

$2^{\sqrt{2}}, \quad e^{\pi} = i^{-2i}$

2. Если α и β - алгебраические числа, отношение $\frac{\ln \beta}{\ln \alpha}$ определено и иррационально, то это отношение трансцендентно.

$\frac{\ln 3}{\ln 2}, \quad \frac{\ln 4}{\ln_2} = 2.$

Эйлер (гипотеза): *Логарифм алгебраического числа по алгебраическому основанию может быть либо рациональным числом, либо числом трансцендентным.* $\log_2 3 = \frac{\ln 3}{\ln 2}$.

e^{π} (A.O. Гельфонд,1929); $2^{\sqrt{2}}$ (P.O. Кузьмин, 1930);
A.O. Гельфонд (1934) вторая формулировка; Th. Schneider (1934) первая формулировка.

Линейные формы от логарифмов алгебраических чисел

Пусть $\alpha_1, \ldots, \alpha_m$ - алгебраические числа и

$$\Lambda = b_1 \ln \alpha_1 + \cdots + b_m \ln \alpha_m \neq 0, \qquad b_j \in \mathbb{Z}.$$

Проблема: *Найти нетривиальную оценку снизу для величины* $|\Lambda|$ *в зависимости от* $B = \max |b_j|$.

Линейные формы от логарифмов алгебраических чисел

Пусть $\alpha_1, \ldots, \alpha_m$ - алгебраические числа и

$$\Lambda = b_1 \ln \alpha_1 + \cdots + b_m \ln \alpha_m \neq 0, \qquad b_j \in \mathbb{Z}.$$

Проблема: *Найти нетривиальную оценку снизу для величины* $|\Lambda|$ *в зависимости от* $B = \max |b_j|$.

А.О. Гельфонд в период с 1935 по 1949 годы доказал ряд подобных результатов при $m = 2$.

Лучший из них: *Пусть* α, β *– алгебраические числа,* $\Lambda = b_1 \ln \alpha + b_2 \ln \beta \neq 0$, *тогда*

$$|\Lambda| \geq e^{-c(1+\ln B)^{2+\varepsilon}}, \qquad c = c(\varepsilon, \ln \alpha, \ln \beta) > 0.$$

Линейные формы от логарифмов алгебраических чисел

Пусть $\alpha_1, \ldots, \alpha_m$ - алгебраические числа и

$$\Lambda = b_1 \ln \alpha_1 + \cdots + b_m \ln \alpha_m \neq 0, \qquad b_j \in \mathbb{Z}.$$

Проблема: *Найти нетривиальную оценку снизу для величины* $|\Lambda|$ *в зависимости от* $B = \max |b_j|$.

А.О. Гельфонд в период с 1935 по 1949 годы доказал ряд подобных результатов при $m = 2$.
Лучший из них: *Пусть* α, β *– алгебраические числа,* $\Lambda = b_1 \ln \alpha + b_2 \ln \beta \neq 0$, *тогда*

$$|\Lambda| \geq e^{-c(1+\ln B)^{2+\varepsilon}}, \qquad c = c(\varepsilon, \ln \alpha, \ln \beta) > 0.$$

Гельфонд всячески пропагандировал доказательство подобных результатов при $m \geq 3$. Такие оценки, обобщив должным образом метод Гельфонда, впервые получил в 1966г. английский математик A. Baker. За этот результат и его многочисленные приложения в теории чисел Бейкер был удостоен Филдсовской премии.

Алгебраическая независимость чисел

Проблема 1 (А.О. Гельфонд, открыта)

Если $\alpha \neq 0, 1$ *и* β *- алгебраические числа,* $d = \deg \beta \geq 2$, *то числа*

$$\alpha^{\beta}, \ldots, \alpha^{\beta^{d-1}}$$

алгебраически независимы.

Алгебраическая независимость чисел

Проблема 1 (А.О. Гельфонд, открыта)

Если $\alpha \neq 0, 1$ *и* β *- алгебраические числа,* $d = \deg \beta \geq 2$*, то числа*

$$\alpha^{\beta}, \ldots, \alpha^{\beta^{d-1}}$$

алгебраически независимы.

Теорема 2 (Гельфонд, 1949)

Если $\alpha \neq 0, 1$ *- алгебраическое число и* β *- кубическая иррациональность, то* $\alpha^{\beta}, \quad \alpha^{\beta^2}$ *алгебраически независимы.*

Алгебраическая независимость чисел

Проблема 1 (А.О. Гельфонд, открыта)

Если $\alpha \neq 0, 1$ *и* β *- алгебраические числа,* $d = \deg \beta \geq 2$*, то числа*

$$\alpha^{\beta}, \ldots, \alpha^{\beta^{d-1}}$$

алгебраически независимы.

Теорема 2 (Гельфонд, 1949)

Если $\alpha \neq 0, 1$ *- алгебраическое число и* β *- кубическая иррациональность, то* $\alpha^{\beta}, \quad \alpha^{\beta^2}$ *алгебраически независимы.*

Теорема 3 (Diaz,1989, H.,1989)

Если $\alpha \neq 0, 1$ *и* β *- алгебраические числа,* $d = \deg \beta \geq 2$*, то среди чисел* $\alpha^{\beta}, \ldots, \alpha^{\beta^{d-1}}$ *имеется не менее* $\left[\frac{d+1}{2}\right]$ *алгебраически независимых.*

Мультипликативная группа ненулевых элементов поля F_p^* циклическая. Её образующую g легко построить. Решить сравнение $g^x \equiv b \bmod p$ очень трудно, лучшие из известных алгоритмов требуют $O(\exp(c(\ln p)^{1/3}(\ln \ln p)^{2/3}))$ арифметических операций.

Мультипликативная группа ненулевых элементов поля F_p^* циклическая. Её образующую g легко построить. Решить сравнение $g^x \equiv b \bmod p$ очень трудно, лучшие из известных алгоритмов требуют $O(\exp(c(\ln p)^{1/3}(\ln \ln p)^{2/3}))$ арифметических операций. Следующий алгоритм (Диффи и Хеллман, 1976) позволяет двум лицам, общающимся по незащищенному каналу связи, без предварительного обмена секретной информацией выработать общий ключ, который будет известен только им двоим.

Мультипликативная группа ненулевых элементов поля F_p^* циклическая. Её образующую g легко построить. Решить сравнение $g^x \equiv b \bmod p$ очень трудно, лучшие из известных алгоритмов требуют $O(\exp(c(\ln p)^{1/3}(\ln \ln p)^{2/3}))$ арифметических операций. Следующий алгоритм (Диффи и Хеллман, 1976) позволяет двум лицам, общающимся по незащищенному каналу связи, без предварительного обмена секретной информацией выработать общий ключ, который будет известен только им двоим.

Алгоритм 1

Данные: Простое число p, первообразный корень g по модулю p, секретный ключ a абонента A и секретный ключ b абонента B.
Найти: Общий ключ $k \in F_p^*$, известный только абонентам A и B.
1. Абоненту A вычислить $x = g^a$ и передать результат абоненту B.
2. Абоненту B вычислить $y = g^b$ и передать результат абоненту A.
3. Абоненту A положить $k = y^a$,
4. Абоненту B положить $k = x^b$.

Излагаемый здесь алгоритм дискретного логарифмирования ("метод согласования") предложен А.О. Гельфондом в 1962г. Требует $O(p^{1/2} \ln p)$ арифметических операций. В зарубежной литературе называется "методом больших и малых шагов"(Шенкс, 1973).

Излагаемый здесь алгоритм дискретного логарифмирования ("метод согласования") предложен А.О. Гельфондом в 1962г. Требует $O(p^{1/2} \ln p)$ арифметических операций. В зарубежной литературе называется "методом больших и малых шагов"(Шенкс, 1973).

Алгоритм 2

Данные: Простое число $p \geq 3$, *первообразный корень* g *по модулю* p, *число* $b \in \mathbb{Z}$, $p \nmid b$.
Найти: Решение сравнения $a^x \equiv b \pmod{p}$.
1. Вычислить $H = [\sqrt{p}] + 1$.
2. Положить $c = g^H \bmod p$.
3. Составить два набора чисел

$$S_1 = \{c^u \bmod p : 1 \leq u \leq H\}, \quad S_2 = \{bg^v \bmod p : 1 \leq v \leq H\}.$$

4. Упорядочить по возрастанию оба набора S_1 *и* S_2. *Найти совпавшие элементы этих наборов, то есть такие числа* u, v, *для которых*

$$c^u \equiv bg^v \pmod{p}.$$

5. Положить

$$\log b = Hu - v.$$

Наибольшее из известных в настоящее время простых чисел имеет вид $2^{136279841} - 1$. Оно записывается 41024320 десятичными цифрами и было найдено в 2024 году.

Наибольшее из известных в настоящее время простых чисел имеет вид $2^{136279841} - 1$. Оно записывается 41024320 десятичными цифрами и было найдено в 2024 году.
В настоящее время рекордом факторизации является разложение на множители целого числа RSA-250, записываемого 250 десятичными цифрами, 2020 г. Общее время вычислений составило 2700 лет в пересчёте на один процессор частотой 2,1 ГГц. В вычислениях участвовали десятки тысяч компьютеров по всему миру. Работа была завершена за несколько месяцев.

Наибольшее из известных в настоящее время простых чисел имеет вид $2^{136279841} - 1$. Оно записывается 41024320 десятичными цифрами и было найдено в 2024 году.
В настоящее время рекордом факторизации является разложение на множители целого числа RSA-250, записываемого 250 десятичными цифрами, 2020 г. Общее время вычислений составило 2700 лет в пересчёте на один процессор частотой 2,1 ГГц. В вычислениях участвовали десятки тысяч компьютеров по всему миру. Работа была завершена за несколько месяцев.
В декабре 2019 года был вычислен дискретный логарифм по модулю 240-значного (795-битного) простого числа. Вычисления заняли примерно 3100 процессорных лет с использованием в качестве эталона процессоров частотой 2,1 ГГц.

Наибольшее из известных в настоящее время простых чисел имеет вид $2^{136279841} - 1$. Оно записывается 41024320 десятичными цифрами и было найдено в 2024 году.
В настоящее время рекордом факторизации является разложение на множители целого числа RSA-250, записываемого 250 десятичными цифрами, 2020 г. Общее время вычислений составило 2700 лет в пересчёте на один процессор частотой 2,1 ГГц. В вычислениях участвовали десятки тысяч компьютеров по всему миру. Работа была завершена за несколько месяцев.
В декабре 2019 года был вычислен дискретный логарифм по модулю 240-значного (795-битного) простого числа. Вычисления заняли примерно 3100 процессорных лет с использованием в качестве эталона процессоров частотой 2,1 ГГц.
В действующих стандартах криптографических алгоритмов используются простые числа размером в 1024 бита или в более важных ситуациях в 2048 битов.