МРНТИ 27.41.23

ИССЛЕДОВАНИЕ ЗАДАЧ ФАКТОРИЗАЦИИ С ИСПОЛЬЗОВАНИЕМ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

У.К. ТУРУСБЕКОВА*, Г.Т. АЗИЕВА

Учреждение «Esil University», Астана, Казахстан,
*E-mail: umut.t@mail.ru

Аннотация. Задача факторизации характерна для широкого спектра математических задач. Решение многих математических задач связано с тем, что результат разложения чисел известен заранее. Данная работа посвящена исследованию задач факторизации с применением эллиптических кривых. Возможность использования таких структур, как эллиптические кривые, с целью факторизации придала новый импульс поиску решения этой проблемы. В статье рассмотрены основные проблемы метода эллиптических кривых, который основан на построении псевдокривой, и возможные пути его оптимизации. Исследованы соотношения между числом сгенерированных кривых и необходимой границей базового метода эллиптических кривых. Исследование данной проблемы выполнено с помощью программной реализации метода, на основе описанного алгоритма для чисел, делители которых не превышают пяти десятичных знаков. Результаты этого исследования представлены для различных случаев начального предела. Полученные результаты указывают на зависимость затрачиваемого времени, конечной границы при процессе факторизации и количества кривых, используемых во время факторизации, от количества кривых после которого увеличивается граница метода эллиптических кривых. В результате анализа этого метода, проведено исследование количества случаев получения делителей составного числа, с помощью дискриминанта кривой.

Ключевые слова: факторизация, эллиптическая кривая, гладкие числа, составные числа, конечное поле, делители числа.

Задача факторизации является частью методов доказательства простоты и псевдопростоты чисел. Необходимость в эффективных методах факторизации вытекает из современной теории моделирования сложных динамических систем, теории построения генераторов псевдослучайных чисел и используется для углубления методов Монте-Карло. Простое, быстрое и доступное мультипликативное разложение составных чисел может стать арифметической операцией, обратной умножению, и таким образом пополнить арсенал математических вычислительных средств.

В результате рассмотрения теоремы Эрдёша-Каца формируется абсолютно новый взгляд на вероятностную теорию чисел. Он связывает распределение различных простых делителей больших чисел с формулами предельных законов теории вероятностей. Согласно этой теореме, для любого целого числа $n \geq 1$, если $\omega(n)-$ это сумма различных простых делителей данного числа, то для любых действительных чисел $a < b$ выполняется

$$\lim_{N\to\infty} \frac{1}{N}\left|\left\{1 \leq n \leq N \mid a \leq \frac{\omega(n)-\log\log N}{\sqrt{\log\log N}} \leq b\right\}\right| = \frac{1}{\sqrt{2\pi}}\int_a^b e^{-x^2/2}dx$$

Это означает, что предельное распределение $\frac{\omega(n)-\log\log N}{\sqrt{\log\log N}}$ соответствует стандартному нормальному распределению. Отсюда следует вывод, что количество натуральных чисел n с небольшим числом делителей увеличивается с ростом значения n.

Задача факторизации также возникает при построении методов решения задачи дискретного логарифмирования [1-2], которая применяется при построении односторонних функций. Эти задачи чрезвычайно важны в компьютерной алгебре и в то же время занимают фундаментальное

положение в современной криптографии. Все современные криптографические системы основаны на том, что существуют односторонние функции и они принадлежат к определенному классу. Все эти факторы в совокупности объясняют чрезвычайную важность и огромный интерес к проблеме факторизации, а также вдохновляют ученых по всему миру на поиск путей ее решения.

Обзор литературы

Решение многих математических задач связано с предположением, что результат разложения чисел известен заранее. Это характерно для таких наук, как математическая теория чисел, теория функций, теория рекурсии в алгебре, теория конечных полей и теория конечных групп. Например, тест на гладкость числа, прежде всего, требует его разложения на простые множители. Дальнейший анализ проводится на основе этой декомпозиции [1]. В работе [1] дается краткое введение в разложение на множители больших целых чисел с помощью алгоритма квадратичного решета. Проблема декомпозиции также возникает для различных быстрых методов многомерного дискретного преобразования Фурье, которые широко используются и имеют существенное значение в теории сигналов [2]. Задача факторизации является частью методов доказательства простоты и псевдопростоты чисел[3]. В работе [3] рассмотрена задача вычисления множества всех первообразных корней произвольного простого числа. В работах [4-5] даны определения субэкспоненциальной сложности. В [6] авторы концентрируются на вычислительных аспектах простых чисел,таких как распознавание простых чисел и обнаружение фундаментальных простых множителей данного числа. Работа [7] посвящена описанию и анализу алгоритма для разложения на множители целых положительных чисел, с использованием эллиптических кривых. В работе [9] показано, что наиболее эффективным способом оптимизации метода эллиптических кривых является использование параллельной реализации с распределеннойпамятью.

Материал и методы исследования

Выбор метода факторизации - довольно простая задача, иногда более сложная, чем сам процесс. Условно все методы можно классифицировать следующим образом:

1. Экспоненциальные методы.
2. Субэкспоненциальные методы.

Эта классификация основана на вычислительной сложности методов.

В случае экспоненциальной сложности сложность задачи ограничена показателем степени многочлена от размера задачи, то есть она ограничена функцией $exp(P(n))$, где P – некоторый многочлен, а n – размер задачи.

Существуют алгоритмы, которые работают более чем за полиномиальное время (“супер-полиномиальное”), но менее чем за экспоненциальное время (“субэкспоненциальное”). К сожалению, строгое определение субэкспоненциальной сложности еще не дано. На данный момент существует два основных определения.

Первое определение: задачу можно решить за субэкспоненциальное время [4].

Второе определение: время выполнения субэкспоненциального алгоритма эквивалентно $2^{O(n)}$ [5]. Это определение допускает большие временные затраты, чем первое. Примером алгоритма с субэкспоненциальным временем является решето общего числового поля для разложения целых чисел на множители.

В случае алгоритмов факторизации субэкспоненциальный характер выражается в L- нотной записи вычислительной сложности. Естественно выбрать наиболее эффективный с точки зрения вычислений метод факторизации. В этом случае очевидно, что экспоненциальные методы можно исключить из рассмотрения, поскольку они намного хуже субэкспоненциальных методов по данному критерию. Однако отказываться от них не следует. При небольшом размере составного числа, которое необходимо разложить на множители, часто более целесообразно использовать экспоненциальные методы.

Среди субэкспоненциальных алгоритмов следует выделить следующие алгоритмы: метод факторизации Диксона, метод факторизации непрерывной дроби, метод квадратичного решета, метод факторизации эллиптической кривой (метод Ленстры) и метод решета числового поля.

В таблице 1 ниже приведены данные о вычислительной сложности каждого метода в L-обозначении.

Таблица 1. Вычислительная сложность методов субэкспоненциальной факторизации

Название метода	Вычислительная сложность
Метод факторизации Диксона	$L_n\left(\frac{1}{2}; 2\sqrt{2}\right)$
Метод разложения непрерывной дроби на множители	$L_n\left(\frac{1}{2}; \sqrt{2}\right)$
Метод квадратичного решета	$L_n\left(\frac{1}{2}; 1\right)$
Метод эллиптической кривой	$L_p\left(\frac{1}{2}; \sqrt{2}\right)$
Метод решета общего числового поля	$L_n\left(\frac{1}{3}; \left(\frac{64}{9}\right)^{\frac{1}{3}}\right)$

Здесь n – составное число, подлежащее разложению на множители, а p – наименьший делитель этого числа.

Существующий метод Ленстры основывается на эллиптических кривых и обеспечивает субэкспоненциальную вычислительную сложность [7]. Рассмотрим данный метод подробно. Напомним, что эллиптическая кривая - это множество решений кубического уравнения, которое записывается в общем виде

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (1)$$

где a_1, a_2, a_3, a_4, a_6 – коэффициенты из поля, по которому строится кривая [8]. Формально, поле представляет собой множество F вместе с двумя операциями, называемыми сложением + и умножением $\times$. Пусть $a, b \in F$, тогда операция - это отображение, которое связывает элемент множества с каждой парой его элементов. Результат сложения $a + b$ называется суммой. Аналогично, результат умножения $a \times b$ называется произведением. Эти операции необходимы для выполнения следующих аксиом поля:

1. Ассоциативность сложения и умножения: $a + (b + c) = (a + b) + c$; $a \times (b \times c) = (a \times b) \times c$
2. Коммутативность сложения и умножения: $a + b = b + a$; $a \times b = b \times a$
3. Аддитивное и мультипликативное тождество: $a + 0 = a$; $a \times 1 = a$
4. Аддитивная инверсия: $a + (-a) = 0$
5. Мультипликативная инверсия: $a \times a^{-1} = 1$

Кольцо - это множество, аналогичное полю, с той разницей, что коммутативность умножения, мультипликативное тождество и обратные аксиомы не выполняются.

Введем понятие эллиптической псевдокривой. Эта кривая определяется условиями:

1. $a, b \in Z_n$;
2. НОД (a, b) =1;
3. НОД($4a^3 + 27b^2, n$)=1;
4. $E_{a,b} = (Z_n) = \{(x, y) \in Z_n \times Z_n : y^2 = x^3 + ax + b\} \vee \{O\}$,

где O – бесконечно соответствующая точка.

Так как F_p не является полем, данная кривая не может быть рассмотрена как эллиптическая кривая.

Рассмотрим алгоритм Померанса [6]:

Входными данными будет составное число n, которое разлагается на простые множители.

1. Выбираем предел первого шага b_1.

2. Генерируем случайную кривую $E_{a,b}(Z_n)$ и точку на ней с координатами (x, y). Более того, $b=\left(y^2-x^3-ax\right)\bmod n$ и $g=НОД\left(n,\ 4a^3+27b^2\right)$. Далее, если g=n, то мы должны вернуться к построению кривой. Если $1<g<n$, то делитель найден.

3. Для любого простого числа $p<b_1$ определим наибольшую степень α_i такую, что $p_i^{\alpha_i}<b_1$. Затем выполним цикл для всех $j=1:\alpha_i$, $P=p_iP$, в результате которого точка P умножается на p^{α_i}. Каждое умножение на p выполняется с использованием алгоритма эллиптического умножения: схема сложения-вычитания [6].

Важным результатом теории эллиптических кривых является теорема Хассе. Согласно этой теореме, верно следующее утверждение: степень $E_{a,b}\left(F_{p^k}\right)$ удовлетворяет неравенству: $p+1-2\sqrt{p}<\left|E_{a,b}\left(F_{p^k}\right)\right|<p+1+2\sqrt{p}$, где $\left|E_{a,b}\left(F_{p^k}\right)\right|$ – количество точек эллиптической кривой или порядок этой кривой [8].

Результаты и обсуждения

Для исследований в предлагаемой статье мы решили использовать стохастическую модель метода эллиптической кривой [9]. Мы реализовали программное обеспечение, которое основан на идее алгоритма Померанса. За входными данные программы были взяты составные числа, которые состояли из произведения двух простых чисел размером $\sim 10^5$. Для каждого случая были применены 10 таких составных чисел, каждое из которых разложили на множители 30 раз. То есть для каждого выбора номера кривых, после которогонеобходимо увеличить границу, было проведено 300 тестов. Были рассмотрены случаи с начальной границей: 100, 30, 6, 2, 1. В процессе исследования такие границы были выбраныс постепенным ускорением программного обеспечения и уменьшением начальной границы.

В качестве количества используемых кривых числа взяли из интервала с шагом 500, затем граница увеличивалась. На 500-м шаге полученные результаты довольно точно описывают общую эффективность метода. Также мы исследовали зависимость времени, затраченного на работу программной реализации, конечной границы и количества используемых кривых. Результаты данного исследования показаны на рисунках 1-3, соответственно.

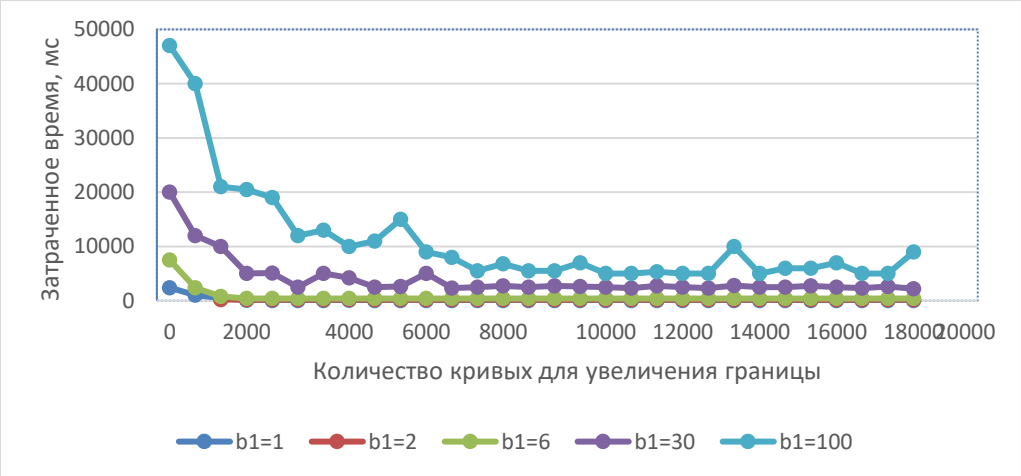

Рисунок 1 – Зависимости затраченного времени от количества кривых

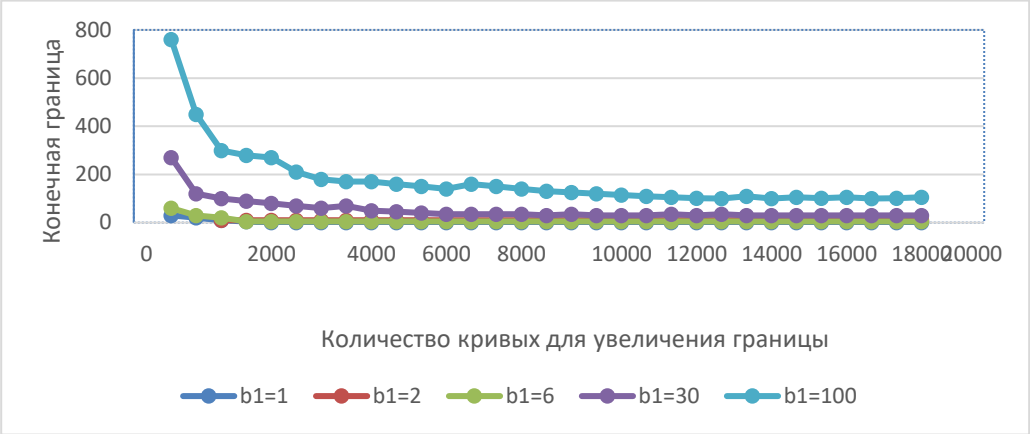

Рисунок 2 – Зависимость конечной границы от количества кривых

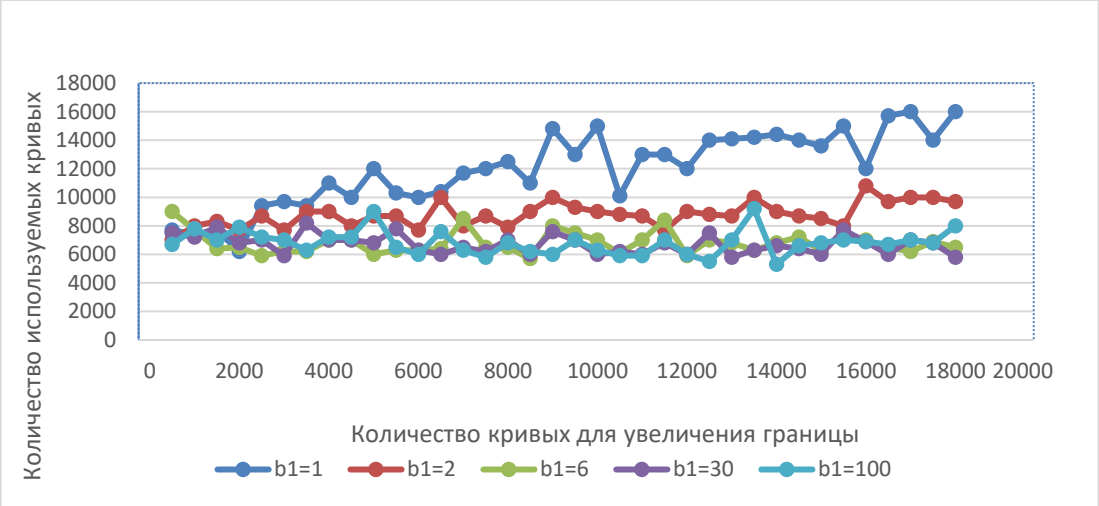

Рисунок 3 –Зависимость количества используемых для факторизации кривых от количества кривых

На всех рисунках мы видим, что увеличение количества кривых, необходимых для изменения границы, привело к снижению временных затрат, а также к уменьшению конечной границы.

Исходя из этого, был подсчитан процент от числа случаев, в которых выполнено второе условие (рис. 4).

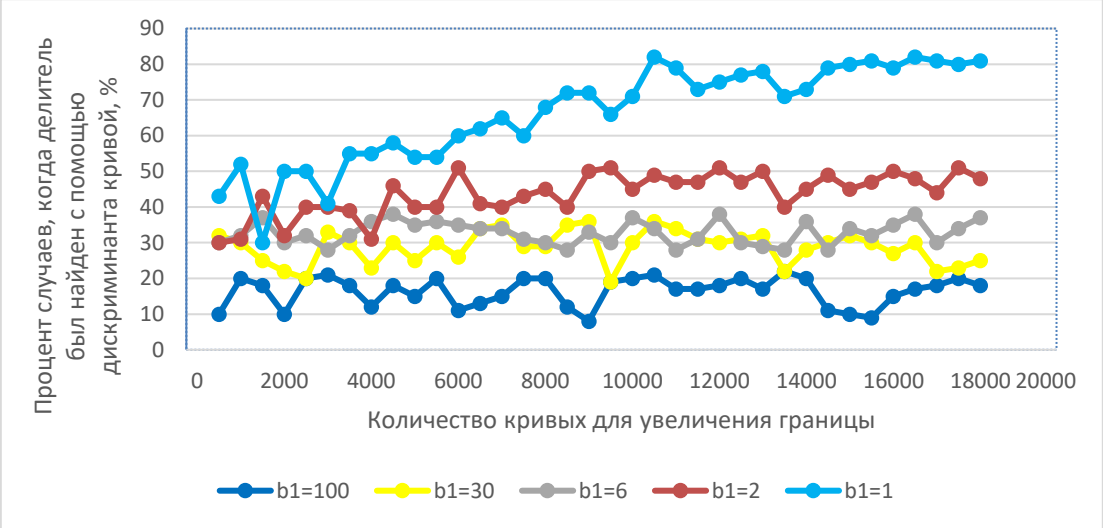

Рисунок 4 –Поиск делителя по дискриминанту зависимости кривойот количества кривых

Основываясь на полученных результатах, можно сделать следующие выводы для чисел, наименьший делитель которых меньше 10^5. Гораздо выгоднее увеличить число кривых, которые применяем, чем границу, чтобы сократить время, необходимое для процесса факторизации, даже в случаях минимальной границы. Более того, наилучшие результаты были получены, когда кривые генерировались до тех пор, пока не возникали подобные ситуации. Таким образом, в тех случаях, когда начальная граница была взята как можно меньше. На это указывают результаты, полученные, когда в качестве начальной границы было взято значение $b_1 = 1$. В данном случае процент таких обращений составил около 80%, а временные затраты были самыми низкими. Это связано со значительным увеличением сложности алгоритма с ростом границы b_1, которое больше, чем с увеличением числа применяемых кривых для заданных составных чисел.

Заключение

Данная работа подчеркивает фундаментальную важность задачи факторизации для ряда как чисто математических, так и прикладных наук. Обоснована фундаментальная важность этой проблемы и ее решения в теории чисел, теории сигналов, современной криптографии, при построении динамических систем и т.д. В статье дана классификация существующих подходов к решению этой проблемы. Особое внимание уделяется проблеме четкого определения “субэкспоненциальной” сложности. Описаны и проанализированы методы субэкспоненциальной факторизации. Обоснована перспективность метода на основе эллиптических кривых, из чего следует значимость этих объектов и их исследования. Показано, что решение, основанное на эллиптических кривых, очень эффективно. В результате теоретического анализа и развития теории эллиптических кривых был построен новый алгоритм. На основе этого алгоритма была разработана программная реализация метода факторизации эллиптической кривой. Процесс разложения на множители был смоделирован для чисел с делителями определенного размера с помощью созданного программного обеспечения. Целью этого процесса было исследование зависимости временных затрат на внедрение программного обеспечения, конечного предела и количества используемых кривых в зависимости от количества кривых, после чего предел автоматически увеличивается. В результате вычислительного анализа алгоритма оказалось, что из-за особенностей эллиптической кривой, построенной над кольцом структуры целых чисел по модулю составных чисел, для чисел малого размера лучше увеличить количество кривых, чем значение границы. Такой подход позволяет значительно сократить временные затраты. Однако

важным моментом является то, что размер делителей составных чиселзаранее неизвестен.

Несмотря на все преимущества данного метода, имеются также пробелы и трудности. Дальнейшие усилия будут направлены на исследование проблемы выбора кривой и влияния этого выбора на процесс факторизации чисел различных классов. Кроме того, важной задачей является исследование дискриминантных признаков кривой, которые позволяют получить разложение составного числа.

Благодарности

Работа выполнена при поддержке Министерства науки и высшего образования Республики Казахстан в рамках проекта AP19677733 «Разработка интеллектуальной распределенной системы параллельного анализа научных текстов», за что авторы выражают огромную благодарность.

Список литературы

1. Pomerance, C. B. Smooth numbers and the quadratic sieve /C. B. Pomerance // Cambridge University Press, New York: Algorithmic Number Theory MSRI Publications, 2008. – V. 44.-P.1–14.

2. Чернов, В. М., Чичева, М. А. Алгебро-арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований/ В. М. Чернов, М. А. Чичева. - Самара: Изд-во СГАУ, 2010. – 102 с.

3. Турусбекова У.К., Муратбеков М.М., Алтынбек С.А., Ахатова Ж.Е. Исследование свойств структур рекурсивных циклов первообразных корней // Вестник КазНПУ им. Абая, серия «Физико - математические науки», 2023. - №83(3). С.59-66. doi: https://doi.org/10.51889/2959-5894.2023.83.3.007.

4. Complexity Zoo., Wayback Machine Class SUBEXP: Deterministic Subexponential-Time,2008. https://complexityzoo.uwaterloo.ca/Complexity_Zoo:S#subexp.

5. Regev, O. A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problemwith Polynomial Space, 2004. https://arxiv.org/abs/quant-ph/0406151.

6. Crandall, R. E., Pomerance, C. B. Prime numbers: A Computational Perspective/ R. E. Crandall, C. B. Pomerance // Springer-Verlag, New York, 2001.- P. 293–420.

7. Lenstra, H. W. Factoting integerswith elliptic curves/ H. W. Lenstra // Annual of Mathematics, New-Jersey, 1987.- V. 126.- P. 649–673.

8. Ишмухаметов, Ш.Т. Методы факторизации натуральных чисел/Ш.Т. Ишмухаметов-Казань: Казанский университет, 2011. -190 с.

9. Ефимов, С.С., Макаренко, А.В., Пыхтеев, А.В. Параллельная реализация исравнительный анализ алгоритмов факторизации в системах с распределённой памятью/ С.С. Ефимов, А.В. Макаренко, А.В. Пыхтеев//Омский государственный университет им. Ф.М. Достоевского, Математические структуры и моделирование, 2012. - №26.- С.94-109.

References

1. Pomerance, C. B. (2008). Smooth numbers and the quadratic sieve. CambridgeUniversity Press, New York: Algorithmic Number Theory MSRI Publications, 44, 1–14.

2. Chernov, V. M. and Chicheva, M. A. (2010). *Algebraicheskie arifmeticheskie metody dlya sinteza bystryh algoritmov diskretnyh ortogonalnyh preobrazovanij*, (Samara: Izd-vo SGAU), 102 p. (in Russ.)

3. Turusbekova U., Muratbekov M., Altynbek S. and Akhatova Zh. (2023) Issledovaniye svoystv struktury rekursivnykh tsiklov pervoobraznykh korney. Vestnik KazNPU im. Abaya, seriya «Fiziko-matematicheskiye nauki», 83(3). 59-66. (in Russ.) doi: https://doi.org/10.51889/2959-5894.2023.83.3.007.

4. Complexity Zoo. (2008). Wayback Machine Class SUBEXP: Deterministic Subexponential-Time. https://complexityzoo.uwaterloo.ca/Complexity_Zoo:S#subexp.

5. Regev, O. (2004). A subexponential time Algorithm for the Dihedral Hidden Subgroup Problem

with Polynomial Space https://arxiv.org/abs/quant-ph/0406151.

6. Crandall, R. E. and Pomerance, C. B. (2001). Prime numbers: A Computational Perspective, Springer-Verlag, New York, pp. 293–420.

7. Lenstra, H. W. (1987). Factoting integerswith elliptic curves, Annual of Mathematics, New-Jersey, 126, 649–673.

8. Ishmukhametov, Sh. T. (2011). *Metody faktorizacii naturalnyh chisel*, (Kazan: Kazanski universitet), 190 p. (in Russ.)

9. Efimov, S. S., Makarenko, A. V. and Pykhteev,A.V. (2012). Parallel'naya realizatsiya isravnitel'nyy analiz algoritmov faktorizatsii sraspredelennoy pamyat'yu, Omskiy gosudarstvennyy universitet im. F.M. Dostoyevskogo, Matematicheskiye struktury i modelirovaniye, Omsk, **26**, 94–109. (in Russ.)

ЭЛЛИПТИКАЛЫҚ ҚИСЫҚТАРДЫ ҚОЛДАНУ АРҚЫЛЫФАКТОРИЗАЦИЯ ЕСЕПТЕРІН ЗЕРТТЕУ

У.К. ТУРУСБЕКОВА*, Г.Т. АЗИЕВА

«Esil University» мекемесі, Астана, Қазақстан
*E-mail: umut.t@mail.ru

Аңдатпа. Факторизация мәселесі математикалық есептердің ауқымды спектріне тән. Көптеген математикалық есептерді шешу сандардың жіктелуінің нәтижесі алдын-ала белгілі болуымен байланысты. Бұл жұмыс эллиптикалық қисықтарды қолдана отырып, факторизация есептерін зерттеуге арналған. Эллиптикалық қисықтар сияқты құрылымдарды факторизациялау мақсатында пайдалану мүмкіндігі бұл мәселенің шешімін табуға жаңа серпін берді. Мақалада жалған қисық құруға негізделген эллиптикалық қисық әдісінің негізгі мәселелері және оны оңтайландырудың мүмкін жолдары қарастырған. Жасалған қисықтар саны менэллиптикалық қисықтардың негізгі әдісінің қажетті шекарасы арасындағы қатынастар зерттелді. Бұл мәселені зерттеу бөлгіштері бес ондық таңбадан аспайтын сандар үшін сипатталған алгоритм негізінде әдісті бағдарламалық қамтамасыз ету арқылы жүзеге асырылады. Бұл зерттеудің нәтижелері бастапқы шектің әртүрлі жағдайлары үшін берілген. Нәтижелер факторизация процесінде жұмсалған уақыттың, соңғы шекараның және факторизация кезінде қолданылатын қисықтар санының қисықтар санына тәуелділігін көрсетеді, содан кейін эллиптикалық қисықтар әдісінің шекарасы артады. Осы әдісті талдау нәтижесінде қисық дискриминанттықолдана отырып, құрама санның бөлгіштерін алу жағдайларының саны зерттелді.

Түйін сөздер: факторизация, эллиптикалық қисық, тегіс сандар, құрама сандар, ақырлы өріс, санның бөлгіштері.

RESEARCH OF FACTORIZATION PROBLEMS USING ELLIPTIC CURVES

U.K. TURUSBEKOVA, G.T. AZIEVA

Institution "Esil University", Astana, Kazakhstan
*E-mail: umut.t@mail.ru

Abstract. The factorization problem is typical for a wide range of mathematical problems. The solution of many mathematical problems is due to the fact that the result of the decomposition of numbers is known in advance. This work is devoted to the study of factorization problems using elliptic curves. The possibility of using structures suchas elliptic curves for the purpose of factorization has given a new impetus to the search for a solution to this problem. The article discusses the main problems of the elliptic curve method, which is based on the construction of a pseudo- curve, and possible ways to optimize it. The relations between the number of generated curves and the necessary boundary of the basic elliptic curve method are investigated. The study of this problem was carried out using a software implementation of the method based on

the described algorithm for numbers whose divisors do not exceed five decimal places. The results of this study are presented for various cases of the initial limit. The results obtained indicate the dependence of the time spent, the final boundary during the factorization process and the number of curves used during factorization on the number of curves after which the boundary of the elliptic curve method increases. As a result of the analysis of this method, a study was conducted on the number of cases of obtaining divisors of a composite number using a curve discriminant.

Keywords: factorization, elliptic curve, smooth numbers, composite numbers, finite field, number divisors.