На правах рукописи

Зиятдинов Дмитрий Булатович

Разработка и оценка эффективности алгоритмов просеивания для факторизации натуральных чисел

Специальность 01.01.06 — Математическая логика, алгебра и теория чисел.

Автореферат

диссертации на соискание учёной степени

кандидата физико-математических наук

Казань — 2012

Работа выполнена на кафедре системного анализа и информационных технологий государственного автономного образовательного учреждения высшего профессионального образования «Казанский (Приволжский) федеральный университет»

Научный руководитель:	доктор физико-математических наук, профессор ФГАОУВПО «Казанский (Приволжский) федеральный университет» Ишмухаметов Шамиль Талгатович
Официальные оппоненты:	доктор технических наук, профессор КГТУ (КАИ) им. А.Н. Туполева Захаров Вячеслав Михайлович
	кандидат физико-математических наук, доцент ФГАОУВПО «Казанский (Приволжский) федеральный университет» Фролов Андрей Николаевич
Ведущая организация:	Ульяновский государственный университет

Защита состоится «29» марта 2012 г. в 16^{30} часов на заседании диссертационного совета Д 212.081.24 при ФГАОУВПО «Казанский (Приволжский) федеральный университет» по адресу: 420008, г. Казань, ул. Кремлевская, д. 35, конференц-зал научной библиотеки им. Н.И. Лобачевского.

С диссертацией можно ознакомиться в научной библиотеке им. Н.И. Лобачевского.

Автореферат разослан « » февраля 2012 года.

Ученый секретарь
диссертационного совета,
к. ф.-м. н., доцент Еникеев А.И.

Общая характеристика работы

Актуальность темы:

Задача целочисленной факторизации состоит в разложении произвольного натурального числа n на простые множители. Она относится к классу трудных задач, но на сегодняшний день теоретически не доказана принадлежность факторизации ни к классу сложности P, ни NP (см., например, [24], с.336). Напомним, что в недавней работе [6] показано, что задача определения простоты числа лежит в P, а значит существует детерминированный алгоритм, за полиномиальное время от длины поданного на его вход целого числа определяющий, является ли оно простым или нет. В то же время на практической трудоемкости решения задачи факторизации с помощью современных вычислительных средств в настоящее время основывается чрезвычайно широко распространенный метод шифрования с открытым ключом RSA, а также некоторые алгоритмы цифровой подписи.

Существование классического алгоритма, решающего задачу факторизации за полиномиальное время, заставило бы полностью отказаться от RSA в будущем, и скомпрометировало бы большое количество уже существующих систем. Однако, самый быстрый алгоритм факторизации произвольных натуральных чисел, известный на сегодняшний день, имеет субэкспоненциальную оценку времени работы. Это значит, что он работает медленнее полиномиального, но все-таки значительно быстрее экспоненциального. Благодаря этому приемлемый уровень безопасности в схеме шифрования RSA достигается при использовании ключей достаточно небольшого размера. Но прогресс в области компьютерных технологий и алгоритмов факторизации постоянно увеличивает нижнюю границу размера для ключа, который считался бы на текущий момент безопасным.

Согласно отчету о последнем достигнутом рекорде факторизации (см. [17]), который был установлен 12 декабря 2009 г., с помощью алгоритма решета числового поля на простые множители было разложено 768-битное 232-значное число RSA-768. Общее потраченное на выполнение этой работы время составило два с половиной года. При этом распределенные вычисления на сотнях компьютеров потребовали более 10^{20} операций, что эквивалентно 2000 годам вычислений на компьютере класса 2.2GHz AMD Opteron. Однако авторы исследования справедливо оценивают затраченные усилия по факторизации 768-битного модуля как достаточно малые, чтобы рекомендовать больше не использовать модули такого размера даже для кратковременной защиты данных. Кроме того, выдвигается предположение, что факторизация 1024-битного RSA модуля, хоть и будет примерно в тысячу раз более слож-

ной задачей, но ее решение, в рамках схожего академического проекта, может быть получено уже в течение следующего десятилетия.

Можно привести следующие аргументы в пользу дальнейшего использования и изучения алгоритмов RSA, а значит и решения задачи факторизации на классическом компьютере:

1. Высокая эффективность RSA на текущий момент, и низкая эффективность альтернативных алгоритмов. Например, устойчивому к взлому с помощью квантового компьютера алгоритму шифрования с открытым ключом Мак-Элис (см. [7]) требуется размер ключа порядка $n^2/4 \approx b^2(\log_2 b)^2$ бит. Поскольку допускается, что на момент взлома не существует лучшего алгоритма факторизации, чем алгоритм решета числового поля, и реальный уровень безопасности имеет выглядящий разумным на сегодняшний день порядок $b = 128$, размеры ключей RSA будут исчисляться тысячами бит, в то время как размеры ключей Мак-Элис — миллионами. Также имеет значение скорость работы алгоритма. Алгоритмы цифровой подписи, широко распространенные на текущий момент, допускают подпись и верификацию информации за полиномиальное время. Алгоритмы, устойчивые к возможности взлома на большом квантовом компьютере, работают более медленно. Использование их в настоящее время в сети Интернет повлекло бы за собой существенное снижение производительности сети.

2. Более 20 лет поисков алгоритмов полиномиальной факторизации и безуспешных попыток значительно улучшить асимптотическое время факторизации решета числового поля (см. [16], [14], [12]) позволяют надеяться, что этот алгоритм действительно представляет собой быстрейшую схему факторизации произвольного составного числа на классическом компьютере. Однако, поскольку невыгодно без необходимости увеличивать размер ключа шифрования до бесконечности, а также поскольку алгоритм РЧП обладает сложной структурой, мы полагаем, что все еще возможно локально улучшить его производительность для некоторого класса практически разрешимых задач.

Таким образом, задача исследования классических алгоритмов факторизации является по-прежнему актуальной. Рассматриваемые в диссертации алгоритмы квадратичного решета (КР) и решета числового поля (РЧП) — сложные, состоящие из нескольких этапов, современные алгоритмы, наиболее эффективные для факторизации целых чисел размером от 50 десятичных знаков и более. Одним из важнейших этапов обоих алгоритмов является просеивание — процедура поиска достаточного количества так называемых *гладких чисел* для получения нетривиальной факторизации на последнем этапе.

Как показано в [12] (стр. 268-277, 294-300) эффективность алгоритма факторизации в целом разумно оценивать исходя из того, насколько эффективно возможно выполнить именно этап просеивания. Однако, особенно для алгоритма РЧП, очень важен еще и этап выбора полинома (см. докторскую диссертацию Б.Мерфи, 1999 г. [20] и статью 2004 г. Т.Кляйнюнга [18]).

Отметим, что на сегодняшний день не существует строгого математического обоснования для оценки эффективности работы КР и РЧП в общем случае, все имеющиеся оценки получены при условии ряда эвристических предпосылок. Тем не менее, алгоритмы КР и РЧП достаточно хорошо исследованы. Уже в публикации [23] 1984 г. предлагаются ряд значительных модификаций базового алгоритма КР, без которых эффективное его применение на практике становится уже почти невозможным. Прежде всего это так называемое мультиполиномиальное квадратичное решето (МПКР), позволяющее решать задачу факторизации в параллельных процессах. Подробная публикация [8] 1995 г. описывает важную стратегию просеивания, в результате которой для факторизации могут быть использованы не только найденные гладкие числа (которых в результате однократной работы базового алгоритма может быть найдено недостаточное количество), но и так называемые *полугладкие*. Такая же стратегия применима для алгоритма РЧП. Но еще большее значение имеет сформулированная для РЧП методика решеточного просеивания (см. [16], с.43-49), позволяющая, с помощью особым образом подобранных параметров p, просеивать только выборочные значения полиномов, и при этом получать лишь незначительно меньший выход гладких чисел относительно простого просеивания по всем элементам факторной базы.

В данной работе осуществляется теоретический вывод, обоснование и оценка эффективности одного из возможных алгоритмов просеивания, делающих процедуру факторизации более эффективной — алгоритма просеивания по подинтервалам для КР, а также исследуется процедура выбора эффективного полинома для алгоритма РЧП, связанного с особой областью просеивания. Кроме того исследуется гибридный алгоритм факторизации, полученный с помощью объединения идей КР и РЧП, обнаруживающий при ближайшем рассмотрении большое сходство с алгоритмом, известным как модификация КР Занга (см. [26]). Подобные теоретические обоснования вместе с некоторыми подтверждающими их экспериментальными оценками позволяют получить лучшее представление о границах эффективности процедуры просеивания в алгоритмах КР и РЧП, а значит, в определенном смысле, и об эффективности процедуры факторизации в целом.

Основной целью работы является исследование алгоритмов просеивания в методе квадратичного решета и решета числового поля и оценка их

эффективности, построение оценок для сходимости алгоритма просеивания по подинтервалам.

Для достижения поставленной цели были решены следующие **основные задачи**:

1. Исследованы современные алгоритмы целочисленной факторизации квадратичного решета и числового поля;

2. Построены оценки для частот появления гладких чисел для алгоритма просеивания по подинтервалам, оценена его эффективность относительно стратегии расширения интервала просеивания;

3. Исследованы процедуры выбора эффективных полиномов просеивания для алгоритма решета числового поля;

Основные положения, выносимые на защиту:

1. Разработка алгоритма просеивания по подинтервалам (АПП);

2. Получение оценки выигрыша для выхода гладких при использовании АПП;

3. Разработка программного комплекса для численной проверки полученных оценок;

4. Исследование метода Занга и оценка его эффективности;

5. Разработка алгоритма выбора эффективного полинома для алгоритма решета числового поля и проверка его эффективности;

Методы исследования. При выполнении работы использовались методы теории чисел, теории алгоритмов и компьютерного моделирования;

Научная новизна состоит в решении следующих задач:

1. Разработка и оценка эффективности алгоритма просеивания по подинтервалам, обеспечивающего более эффективный поиск гладких пар в методах целочисленной факторизации квадратичного решета и решета числового поля;

2. Анализ и развитие специального метода Занга целочисленной факторизации;

3. Разработка алгоритма выбора оптимального полинома просеивания в методе решета числового поля;

Практическая значимость: Разработка и анализ алгоритмов просеивания, которые могут быть использованы для построения более эффективных алгоритмов факторизации.

Достоверность изложенных в работе результатов обеспечивается строгостью постановки задач и математических методов их решения, а также системным подходом к разработке и тестированию программного комплекса, экспериментально подтверждающего теоретические оценки.

Апробация работы. Основные результаты работы докладывались на конференциях:

1. Конференция аспирантов и молодых преподавателей КГУ, 2009, Казань
2. 7-я международная научно-практическая конференция «Инфокоммуникационные технологии глобального информационного общества» Казань, 2009;
3. международная школа-конференция молодых ученых – Турку, Финляндия, июнь 2009;
4. научно-практическая конференции и выставка «Инновации РАН – 2010;
5. III Всероссийской научно-практической конференции «Информационные технологии в системе экономической безопасности России и ее регионов», Казань, 2010.

Личный вклад. Автор принимал активное участие в теоретических разработках и анализе предложенных методик, а также разработал и реализовал программные средства, необходимые для получения статистически достоверных численных оценок рассматриваемых в работе алгоритмов.

Публикации. Основные результаты по теме диссертации изложены в 5 печатных изданиях, 2 из которых изданы в журналах, рекомендованных ВАК, 2 — в тезисах докладов.

Объем и структура работы. Диссертация состоит из введения, четырех глав, заключения и приложения. Основной текст диссертации изложен на **86** страницах с **12** рисунками и 10 таблицами. Список литературы содержит **74** наименования.

Содержание работы

Во **введении** обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель, ставятся задачи

работы, сформулированы научная новизна и практическая значимость представляемой работы.

Первая глава посвящена описанию наиболее быстрых из существующих в настоящее время алгоритмов факторизации произвольных больших натуральных чисел — алгоритмов квадратичного решета и решета числового поля. Вводится понятие гладких чисел и другие основные понятия, общие для всех методов факторизации, использующих процедуру просеивания. Обсуждается возможности улучшения оценки времени факторизации в целом и оптимизации отдельных этапов в известных алгоритмах для получения более оптимальных методов. Также вводится стандартная субэкспоненциальная функция сложности $L_n[\alpha, c] = \exp\big((c + o(1))(\ln n)^{\alpha}(\ln \ln n)^{1-\alpha}\big)$, и обсуждаются результаты численных экспериментов, отражающих степень ее адекватности для оценки эффективности факторизации с помощью алгоритмов КР и РЧП на практике.

Класс алгоритмов факторизации, в котором удалось разработать наиболее быстрые на сегодняшний день алгоритмы, в своей основе содержит прием, который был известен еще в 17 в. Пьеру Ферма.

Так, пусть для произвольного нечетного натурального n нам известна такая пара чисел (A, B), что выполняется

$$A^2 - B^2 = n \tag{1}$$

тогда задача факторизации n решается элементарно: $n = (A - B)(A + B)$.

Все алгоритмы факторизации, построенные на этой идее, используют некоторые полиномы, которые в дальнейшем будут называться порождающие полиномы или полиномы просеивания, среди значений которых происходит поиск чисел, которые могут быть использованы для построения выражения вида (1)[1].

Алгоритм факторизации квадратичного решета использует порождающий полином $Q(x) = x^2 - n$, обладающий свойством $Q(x) \equiv x^2 \bmod n$. Это значит, что все значения $Q(x)$ уже являются квадратами по модулю n, и для успешной факторизации достаточно найти некоторое x, для которого $Q(x)$ являлось бы полным квадратом. Однако есть и более эффективный способ: найти среди всех аргументов $Q(x)$ некоторое подмножество S, такое что $\prod_{x \in S} Q(x)$ являлось бы квадратом в $\mathbb{Z}$. Эффективность такого приема связана с открытой в конце 70-х, начале 80-х годов процедурой *просеивания*, позволяющей быстро найти такое подмножество S.

[1]На самом деле используется немного более общее выражение $A^2 - B^2 \equiv 0 \bmod (n)$, тогда, при известных A и B, факторы n находятся как $(A - B, n)$ и $(A + B, n)$

Определение 1. Число называется B-*гладким*, если среди его делителей нет чисел, превосходящих некоторой границы B.

Определение 2. *Просеиванием* полинома по некоторому радиусу L называется процедура, аналогичная процедуре Эратосфенова решета, определяющая какие из значений $Q(x)$, где $x \in [-L; L]$, являются B-гладкими.

Определение 3. Полином, чьи значения исследуются на гладкость в алгоритме факторизации называется *порождающим* полиномом или полиномом просеивания.

Имея в своем распоряжении $B + 1$ гладкое число, всегда возможно найти такое подмножество этих чисел, произведение элементов которого было бы полным квадратом. Таким образом, при заданном B, основная цель алгоритма факторизации сводится к поиску достаточного количества гладких значений порождающего полинома.

Суть процедуры просеивания заключается в следующем. Если для некоторого простого p верно, что $p|Q(x_p) = x_p^2 - n$, то также будет верно, что $p|Q(x_p + kp)$ для любого целого k. Такое свойство порождающего полинома фактически позволяет определить B-гладкость каждого отдельного числа из области значений $Q(x)$ за $O(\ln \ln B)$ шагов (подробнее об этом см. [12], стр.121-131). Просеивание происходит в три этапа: сначала генерируется массив значений $Q(x)$ на некотором интервале $[\lfloor\sqrt{n}\rfloor - L, \lfloor\sqrt{n}\rfloor + L]$, затем для каждого простого p из факторной базы происходит просеивание, то есть элемент массива делится на p, и на последнем этапе происходит поиск элементов массива, обратившихся после процедуры просеивания в единицу; значения $Q(x)$, соответствующие этим элементам и будут искомыми гладкими[2].

Определение 4. *Факторной базой* в алгоритме квадратичного решета называется набор простых чисел, ограниченных сверху некоторой константой B и при этом являющихся квадратичными вычетами по модулю n. Последнее условие необходимо для того, чтобы для любого p из факторной базы сравнение $Q(x) = x^2 - n \equiv 0 \pmod{p}$ имело решение, а значит просеивать по p имело смысл.

[2]Здесь описана самая простая техника просеивания. На практике, для ускорения алгоритма, процедура выглядит несколько иначе: во-первых, переходя к логарифмам значений Q(x), деление можно заменить на вычитание, во-вторых просеивание можно производить «в обратную сторону», то есть инициализировать массив нулями, затем прибавлять $\ln p$ в те места, которые делимы на p для каждого простого p из факторной базы, и на последнем этапе — сравнивать значения элементов массива со средним приближенным значением $\ln Q(x)$. Подробнее об этом см. [12], стр. 123

Задача выбора оптимальных параметров для алгоритмов факторизации (в частности, параметра B) является нетривиальной. Благодаря удачному подбору параметров удается найти достаточное количество гладких чисел за относительно небольшое время от $\ln n$.

Сложность факторизации с помощью алгоритма квадратичного решета при оптимально выбранных параметрах основывается на важной теореме, сформулированной Карлом Померанцем в 1996 г.

Теорема. *(см. [12], стр. 286 и [22], стр. 703–711) Пусть $m_1, m_2, \ldots$ — последовательность целых, равномерно распределенных независимых случайных величин на отрезке $[1..X]$, N — наименьшее целое, такое что в $m_1, m_2, \ldots m_N$ существует подпоследовательность, произведение элементов которой является квадратом. Тогда ожидаемое значение N выражается формулой: $L(X)^{\sqrt{2}+o(1)}$, где $L(X) = exp(\sqrt{\ln X \ln\ln X})$. Кроме того, ожидаемое значение N не изменится, если потребовать, чтобы каждое из чисел m_j в произведении обладало B-гладкостью, где $B = L(X)^{1/\sqrt{2}}$.*

Поэтому сложность алгоритма факторизации КР оценивается выражением $L_n(1/2, 1) = \exp((1 + o(1))\sqrt{\ln n \ln\ln n})$ и такая оценка является лучшей для входных чисел, примерно, от 50 до 100 десятичных знаков[3] (см. [23] для подробного вывода). Из теоремы хорошо видно, почему такая оценка не является абсолютно строгой — предполагается, что числа порождаемые полиномом просеивания в алгоритме будут обладать требуемой степенью гладкости с той же вероятностью, что и независимые равномерно распределенны случайные величины.

Алгоритм решета числового поля, имеет таким же образом полученную теоретическую оценку сложности

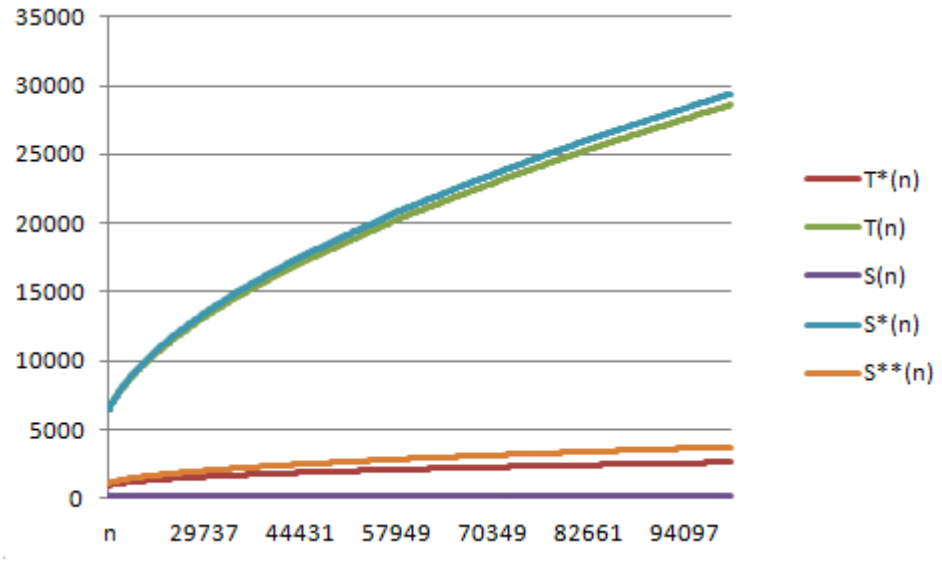
$$L_n(1/3, c) = \exp((c + o(1))(\ln n)^{1/3}(\ln\ln n)^{2/3} \tag{2}$$

где $c \approx 1,92$, которая, конечно же, асимптотически значительно лучше, чем оценка полученная для алгоритма квадратичного решета. Однако в остальном алгоритм РЧП лишь развивает описанные выше идеи, используя более общее понятие гладкости и позволяя, кроме того, более гибко выбирать параметры, но не вносит существенных изменений в основные этапы процедуры факторизации.

Далее, с помощью описанного в тексте диссертации численного эксперимента показано, что асимптотическая оценка времени работы алгоритма решета числового поля действительно отражает фактическую сложность факторизации даже для небольших n, однако при этом значительную роль

[3] Общий вид функции $L_n[\alpha, c] = \exp\left((c + o(1))(\ln n)^{\alpha}(\ln\ln n)^{1-\alpha}\right)$, причем $o(1) \to 0$, только если $n \to \infty$.

Рис. 1: Сравнение оценок сложности алгоритмов КР и РЧП для небольших чисел



играет оптимальный выбор всех параметров. Более того, на практике уменьшение или увеличение значения константы c и даже слагаемого $o(1)$ в выражении (2) также будет вносить существенный вклад в сложность алгоритма.

Пусть $L_n(\eta) = exp\left((1+\eta)\sqrt{\ln n \ln\ln n}\right)$ — оценка сложности факторизации методом КР с учетом константы η. На рис. 1 отображены $S(n) = L_n(0)$, $S^{**}(n) = L_n(0,55)$ и $S^{*}(n) = L_n(0,94)$. Видно, что, хоть $S(n)$ в этом случае выглядит значительно предпочтительнее всех прочих оценок, уже $S^{**}(n) = L_n(0,55)$ сравнима по величине с асимптотически оптимальной функцией сложности РЧП — $T^{*}(n) = \exp\left(1,92 \cdot (\ln n)^{1/3}(\ln\ln n)^{2/3}\right)$, а $S^{*}(n) = L_n(0,94)$ практически совпадает с эмпирически выведенной функцией сложности РЧП для малых n и оптимальных начальных параметрах — $T(n)$.

Во **второй главе** теоретически выводится, анализируется, получает теоретическую и экспериментальную оценки методика просеивания по подинтервалам.

Рассматрим ситуацию, когда процедура просеивания завершила свою работу. Результат ее работы — множество пар

$$S = \{(A,B):\ A = x+m,\ B = q(x)\}, \tag{3}$$

удовлетворяющих условию $A^2 \equiv B \bmod n$, где B обладает свойством гладкости. Далее это множество должно быть отфильтровано так, чтобы остались лишь пары (A,B), для которых НОД$(A,\ B) = 1$.

Часто бывает, что размер множества S после фильтрации становится значительно меньше размера факторной базы. Итак, нужно совершить дополнительную работу для поиска новых гладких чисел. Это тем более вероятно,

что потенциально отфильтровано может быть также большое количество пар, для которых B хоть и является гладким, но не может быть использовано для получения искомого соотношения конгруэнтности двух квадратов по модулю n (это такие B, которые содержат в качестве произведения простое число p, не содержащееся ни в одном другом B из S).

Предлагается теперь вместо увеличения радиуса просеивания L или изменения границы B наибольшего простого в FB произвести дополнительный поиск гладких среди значений полиномов $q_p(k) = q(x + pk)/p$, где $q(x) = 0 \pmod{p}$.

Определение 5. *1-гладким* называют число z, если оно является произведением гладкого числа r и простого p, меньшего чем $B_1 = B^2$.

После завершения первого этапа просеивания находится также большое количество *1-гладких* чисел. Если для некоторого x значение $q(x)$ будет *1-гладким*, то есть $q(x) = r \cdot p$, где $B < p < B_1$, то каждое последующее значение $q(x + p \cdot k)$ также делимо на p для всех $k \in \mathbf{Z}$. Запишем многочлен $q(x + p \cdot k)$ в виде:

$$q(x + p \cdot k) = (x + p \cdot k)^2 + 2m(x + p \cdot k) - a = q(x) + p^2k^2 + 2pk(x + m).$$

Обозначим через $q_p(k)$ последнее выражение, поделенное на p:

$$q_p(k) = q(x + p \cdot k)/p = pk^2 + 2k(x + m) + r, \tag{4}$$

так как $q(x) = p \cdot r$.

Несложно показать, что скорости роста функций $q(x)$ и $q_p(k)$ приблизительно совпадают, если p невелико. Таким образом, мы получаем новый объект для просеивания. Так как просеивание полинома (4) эквивалентно просеиванию исходного полинома $q(x)$ по аргументам $x_k = x + p \cdot k$, методика получила название *просеиванием по подинтервалам.*

Заметим, что на возможность такого просеивания указывается в одной из ранних статей Померанца о методе квадратичного решета ([23], с.6-7), однако без детального анализа алгоритма, его ограничений и приемуществ. Просеивание по подинтервалам перекликается также со стратегией решеточного просеивания в методе решета числового поля, которая была предложена Дж.Поллардом в [16], с.43-49, и, частично, с идеей поиска полугладких чисел (Боендер, [8]), однако полностью не повторяет ни одну из них. В работе осуществляется вывод теоретических оценок, подтверждающих эффективность методики просеивания по подинтервалам, а также приводятся результаты численного эксперимента на большом объеме данных.

Сформулирована и доказана следующая теорема.

Теорема 1. *Если на некотором интервале L, полином просеивания $q(x)$ ограничен сверху некоторой константой M, то эффективность просеивания по одному дополнительному подинтервалу для $p \approx B$ относительно просеивания по двукратному расширению исходного интервала можно оценить формулой:*

$$\frac{\rho\left(\frac{\ln M(1+1/B)+(B-1)L^2+2BL-a}{\ln B}\right)}{2\rho\left(\frac{\ln 2M+8L^2-a}{\ln B}\right)-\rho\left(\frac{\ln M}{\ln B}\right)}\cdot 100\% \tag{5}$$

где $\rho(u)$ – функция Дикмана де-Брюина. Причем наибольший выигрыш в выходе гладких на подинтервале будет достигаться при условии $2B = L$.

Следствие. *Для того, чтобы просеивание по подинтервалам было эффективно, достаточно чтобы выполнялось условие $L^3 + 16L^2 < 2M$.*

Вследствие проведенного численного эксперимента удалось показать, что выигрыш в среднем от использования методики просеивания по подинтервалам в алгоритме КР, при условии достаточно хорошо подобранных исходных параметров[4] достигает от 20% до 50%. Следующие графики отражают этот выигрыш как относительный прирост в выходе гладких при использовании гладких найденных на исходном интервале и подинтервалах, относительно прироста гладких, получаемого вследствие увеличения исходного интервала просеивания в два, три и четыре раза.

Также в работе рассматривается применение методики просеивания по подинтервалам к специальному виду алгоритма КР, который называется вариацией Занга ([26], стр. 3-4). Анализ показывает низкую эффективность методики для полиномов просеивания, степень которых $r > 2$.

Итак, методика просеивания по подинтервалам может очень эффективно использоваться как в алгоритме квадратичного решета, так и в его модификациях, для получения выигрыша при поиске гладких чисел, причем численный эксперимент показывает стабильность этого выигрыша при росте n. Однако эффективность методики быстро падает с ростом степени полинома просеивания. В методе решета числового поля похожий подход носит название решеточного просеивания, однако они не идентичны. Приведенные теоретические и экспериментальные оценки уточняют на какой именно выигрыш можно рассчитывать, применяя данную методику и очерчивают границы ее эффективного применения в том или ином алгоритме факторизации.

[4]Параметрами в данном случае были полином $Q(x) = (m+x)^2 - n$, граница поиска гладких B и радиус просеивания L.

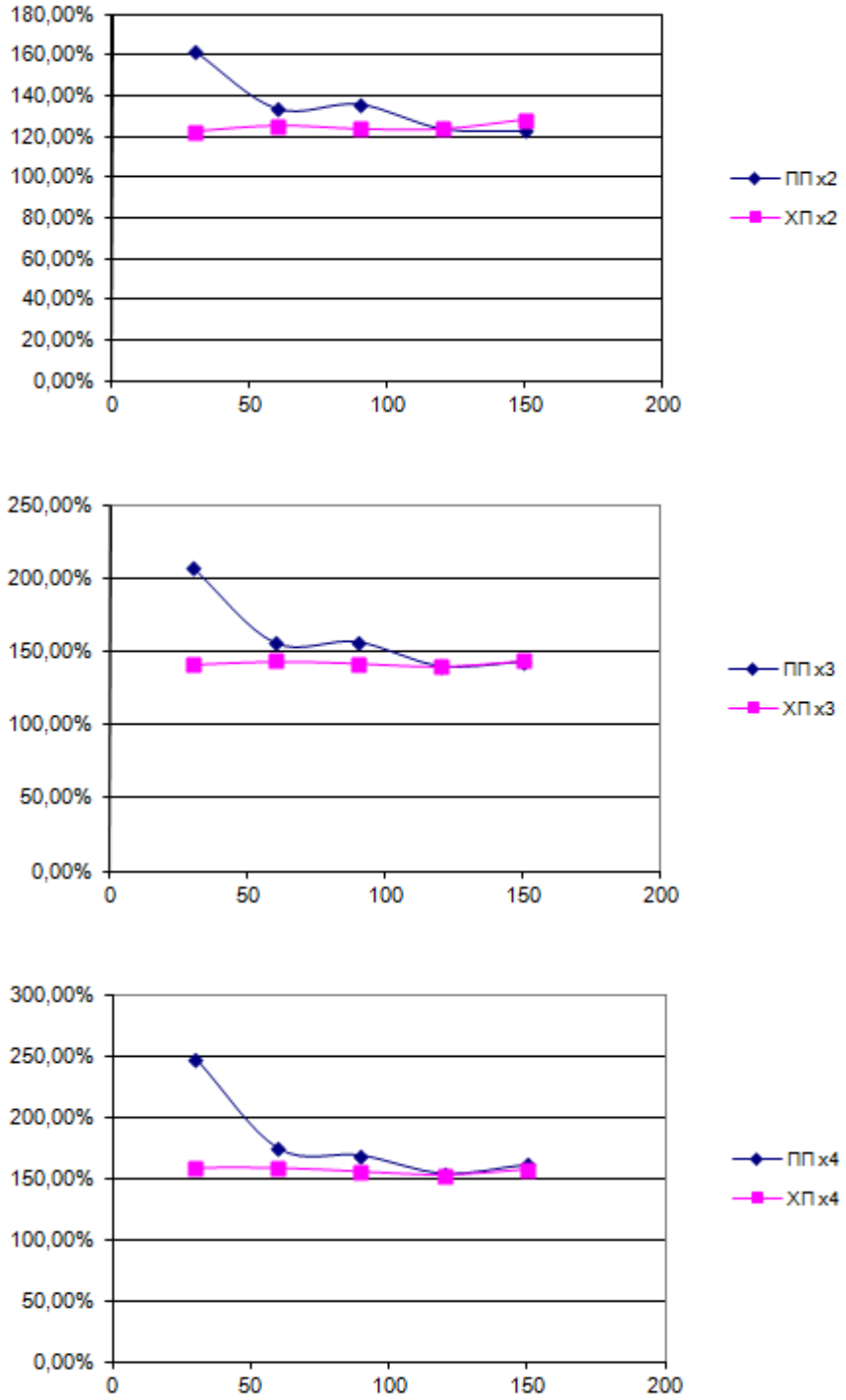


Рис. 2: Относительный выигрыш от методики просеивания по подинтервалам в алгоритме квадратичного решета для равномощных классов "хороших"исходных полиномов (ХП) и "плохих"исходных полиномов (ПП) для чисел длины от 60 до 150 бит.

В **третьей главе** рассматривается общая методика, позволяющая сделать алгоритмы факторизации более эффективными за счет просеивания значений порождающего полинома по области особого вида. Сначала строится и анализируется гибридный метод факторизации, совмещающий в себе идеи алгоритмов КР и РЧП, доказывается утверждение об эффективности просеивания в таком алгоритме вдоль оптимальной прямой. Затем осуществляются теоретические построения, связывающие методику просеивания по особой области с процедурой выбора оптимального полинома для алгоритма решета числового поля. В конце приводятся результаты численного эксперимента, эмпирически доказывающего эффективность описываемой методики для кубических полиномов просеивания в РЧП и чисел n длины порядка 120-бит.

В гибридном методе факторизации предлагается сначала, так же как и в методе РЧП сначала выбирать неприводимый в поле рациональных чисел $\mathbb{Q}$ многочлен $P(x)$ степени $r \geq 2$ с целыми коэффициентами. На следующем этапе РЧП предполагает просеивание многочленов вида $a + bx$ по алгебраической факторной базе, состоящей из простых идеалов вида $a + b\theta$ в кольце $\mathbb{Z}[\theta]$, где θ — комплексный корень многочлена $P(x)$ с одновременным просеиванием чисел $a + bm$ по рациональной базе.

В гибридном методе предлагается отказаться от просеивания по алгебраической факторной базе, рассматривая в качестве множества для просеивания по рациональной базе числа специального вида $a + bm$, где a и b подобраны так, что многочлен $a + bx$ является квадратичным вычетом по модулю многочлена $P(x)$.

При таком подходе алгебраическая факторная база не нужна вообще, и двучлены $a + bx$, рассматриваемые здесь, автоматически будут полными квадратами по модулю $P(x)$ в силу выбора (a, b). Просеивание будет проводиться только по рациональной базе, которая выбирается обычным образом.

Пусть $P(x) = x^2 + cx + d$ — квадратичный полином[5], $a + b\,x = Q^2(x) \bmod P(x)$, тогда $Q_{a,b}(x) = (a + bx)^2 \bmod P(x) = (a^2 - b^2 d) + (2ab - b^2 c)x = a_1 + b_1 x$. Теперь обозначим $F(a, b) = Q_{a,b}(m) \bmod P(m)$, тогда $F(a, b)$ всегда будет квадратом в $\mathbf{Z}/\mathbf{NZ}$.

$$F(a, b) = Q_{a,b}(m) = a_1 + b_1 m \bmod N. \tag{6}$$

[5]В случае кубического полинома $P(x)$ данный метод преобразуется в не очень эффективный метод квадратичного решета в вариации Занга [26]. Как показано в [19] эффективно использовать подобную же методику для степеней $P(x)$ $r > 3$ скорее всего невозможно. Опять же, литература по данным методикам крайне малодоступна и не отражает весь спектр их возможных применений

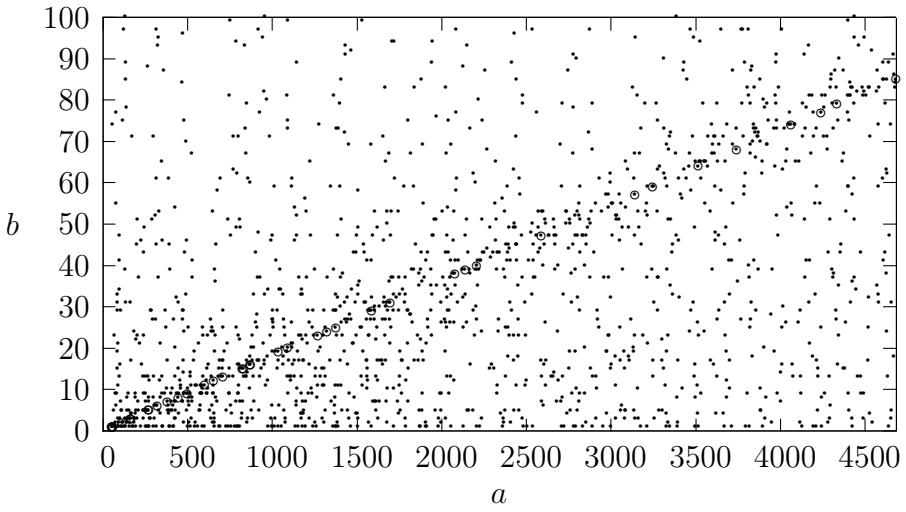


Рис. 3: Распределение гладких пар вдоль оптимальной прямой

Для оценки роста значений функционала $F(a, b, m)$ заметим, что наименьшее значение он достигает в начале координат $a = 0$, $b = 0$ и на прямых

$$a = tb$$

где t — корень многочлена $W(t) = t^2 + 2mt - cm - d$.

Поскольку, коэффициенты a и b принимают только целые значения, а значения корня t иррациональны (иначе, мы бы имели нетривиальное разложение числа N), то точного значения достичь невозможно. Пусть t — один из корней полинома $W(t)$. Будем называть прямую $a = t\,b$ *оптимальной*.

Утверждение 1. Значение функционала $F(a, b)$ в точках (a_0, b_0), примыкающих к оптимальной прямой $a = t\,b$ прямо пропорционально аргументу b_0 с коэффициентом пропорциональности, равным примерно $1, 2m$.

Другими словами, функционал $F(a, b)$ изменяется линейно вдоль линии $a = t\,b$.

Рис.1 демонстрирует распределение гладких значений $F(a, b, m) = b^2 W(t)$ на примере $N = 1439 \cdot 1747 = 2513933, m = 1531, P(x) = x^2 + 111x + 3, W(t) = t^2 + 3062t - 169972, t_0 \approx 54, 54$. Размер факторной базы — 30 элементов. Кружочками обведены пары, найденные в результате просеивания по области $(a, b) \in [(54b - 10...54b + 10) \times (1...100)]$.

Этот метод очень близко смыкается с методом квадратичного решета. Действительно, просеивание в методе квадратичного решета выполняется по последовательности $Q(a) = (\lfloor\sqrt{N}\rfloor + a)^2 - N \approx a^2 + 2a\sqrt{N}$ для $a \in \{\pm 1, \pm 2, \pm 3, ...\}$. Поскольку, параметр m при $r = 2$ равен примерно

$[\sqrt{N}]$, то можно считать просеивание по методу квадратичного решета частным случаем формул (6) при $a_1 = a^2$, $b_1 = 2a$.

Отличие заключается в том, что теперь мы можем просеивать по области особого вида, минимизирующей рост полинома $Q(a)$. Это позволяет, просеивая равное количество элементов, найти до 6 раз большее количество гладких пар по сравнению с обычным КР.

Ту же идею можно применить для алгоритма решета числового поля.

В статье Кляйнюнга [18] предложен метод построения пары полиномов с целыми коэффициентами $F_1(x) = p^d(a_d x^d + a_{d-1}x^{d-1} + ... + a_1 x + a_0)$ и $F_2(x) = px - m$, имеющих общий корень m/p по модулю n, где n — это число, которое требуется факторизовать, p — целое число. То есть выполняется:

$$F_1(\frac{m}{p}) = n, \tag{7}$$

$$F_2(\frac{m}{p}) = 0.$$

В указанной статье на выбор числа p не накладывается никаких условий, кроме:

1. $p \ll m$;
2. p представляет собой произведение нескольких небольших простых чисел.

Выбор пары полиномов в методе Кляйнюнга выполняется неоднозначно, а критерием оценки качества полинома является некоторая мера, представляющую собой функционал, значение которого определяется коэффициентами полинома и действительным числом k, называемым skewness. В результате выбор полиноминальной пары сводится к перебору всевозможных полиномов $F_1(x)$, удовлетворяющих условию (7), и выбору среди них полинома с наименьшей мерой. Второй полином определяется однозначно параметрами p и m. Такой подход не оптимален и обладает тем недостатком, что время его работы для больших n слишком велико (полгода для подбора подходящего полинома в рекордном разложении 768-битового числа n, см [17]).

В диссертации предлагается другой подход к выбору полинома $F_1(x)$. Наша идея заключается в том, чтобы выбирать полином $F_1(x)$ так, чтобы его производная $F_1'(x)$ имела два действительных корня α_1 и α_2, расположенных недалеко друг от друга, причем полином $F_1(x)$ в точках α_1 и α_2 имел противоположные значения, тогда $F_1(x)$ имеет действительный корень между α_1 и α_2:

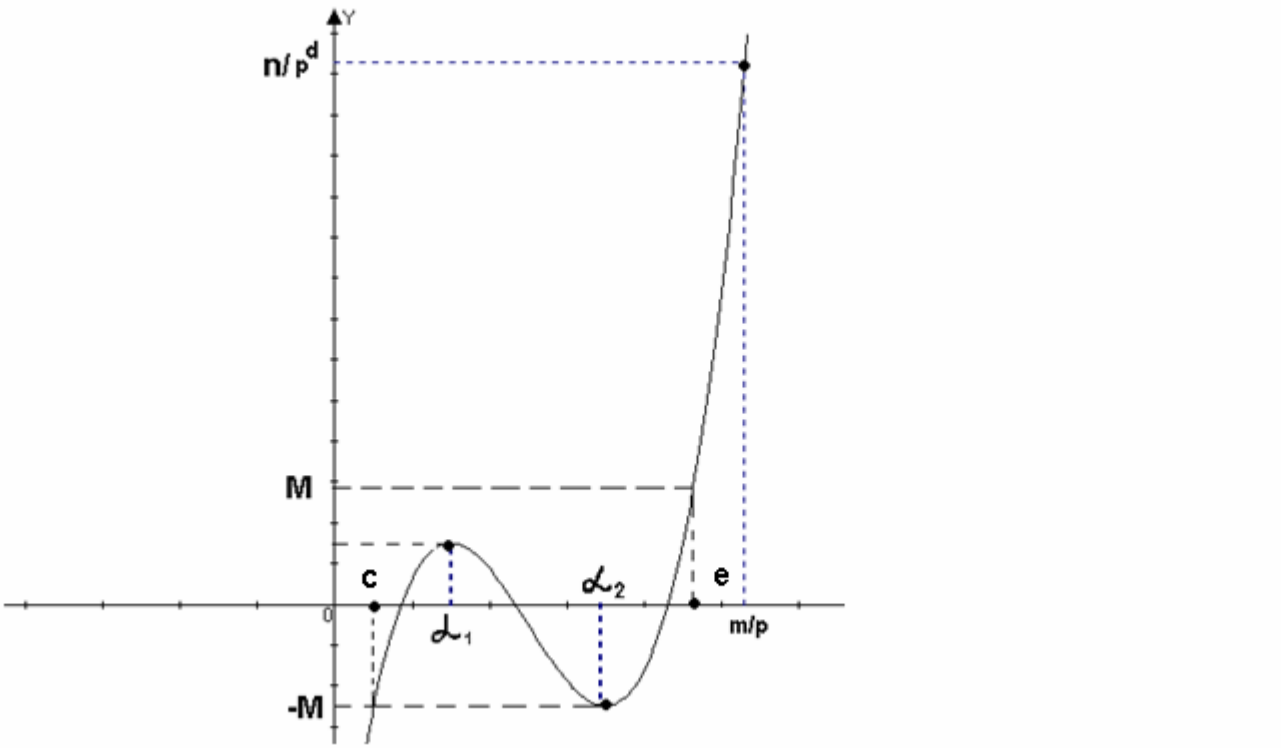


Рис. 4: График полинома $F_1(x)$ с корнями производной α_1 и α_2

Пусть $M = \max(|F_1(\alpha_1)|, |F_1(\alpha_2)|)$. Рассмотрим наибольший непрерывный интервал [c, e], содержащий точки α_1 и α_2 на котором выполнено неравенство $|F_1(x)| \leq M$ (см. рис. 4). Обозначим через x_0 корень $F_1(x)$, находящийся между точками α_1 и α_2. По теореме Лагранжа для некоторого ξ_1 в окрестности точки x_0 выполняется $F_1(x) \leq F_1'(\xi_1) \cdot (x - x_0) \leq L \cdot F_1'(\xi_1)$, где L — длина интервала [c, e]. Поскольку точка ξ_1 также находится в окрестности нулей производной $F_1'(x)$, то опять, по теореме Лагранжа, $F_1'(\xi_1) \leq F_1''(\xi_2) \cdot L$, и следовательно $F_1(x) \leq F_1''(\xi_2) \cdot L^2$.

Предположим теперь, что полиномиальная пара $F_1(x)$, $F_2(x)$ выбрана. Для эффективности работы метода РЧП необходимо обеспечить сравнительно небольшие значения нормы линейных полиномов $a - b\theta$ в числовом поле $\mathbb{Z}[\theta]$ [6] при изменении параметров a и b в некоторой области SR (от англ. sieve region). Норма полинома $Nr(a - b\theta)$ может быть вычислена по формуле $Nr(a - b\theta) = b^d F_1(\frac{a}{b})$.

Предположим теперь, что полином $F_1(x)$ имеет свойства, сформулированные выше, и оценим значения нормы $Nr(a - b\theta)$ в специальной области SR, описываемой неравенствами:

$$1 \leq b \leq Q, \;\; c \leq \frac{a}{b} \leq e,$$

[6] θ здесь — комплексный корень $F_1(x)$

где Q — некоторое целое число, а интервал [c, e] выбран как на рис. 4. Эта область представляет собой некоторый сектор ширины L и высоты Q:

$$Nr(a - b\theta) \leq b^d F_1(\frac{a}{b}) \leq Q^d \cdot L \cdot F_1''(\xi_2) \leq Q^d \cdot L \cdot M_1, \tag{8}$$

где M_1 обозначает максимум второй производной на интервале [c, e], L - длина интервала [c, e]. Подсчитаем размер W области SR (количество пар $(a, b) \in SR$):

$W = L + 2L + \ldots + Q \cdot L \approx \frac{1}{2} \cdot L \cdot Q^2$. Найдем из последнего равенства Q и подставим в (8):

$$Q = \left(\frac{2W}{L}\right)^{\frac{1}{2}}, \; Nr(a - b\theta) \leq \left(\frac{2W}{L}\right)^{\frac{d}{2}} \cdot L \cdot M_1 = \sqrt{2^d} \cdot \frac{M_1}{L^{\frac{d}{2}-1}} \cdot W^{\frac{d}{2}} \tag{9}$$

Оценка (9) показывает, что при увеличении площади W сектора SR рост нормы происходит пропорционально $W^d 2$. При изменении ширины L сектора SR без изменения W рост нормы $Nr(a - b\theta)$ будет пропорционален росту полинома $F_1(L)$, т.е. пропорционален L^d.

Значит, в первичном приближении рост нормы будем наименьшим в направлении увеличения высоты Q сектора SR, а не его ширины L. Значит просеивание по сектору с основанием у корней кубического полинома, подобранного таким образом, как это описано выше, должно давать преимущество по сравнению с просеиванием по прямоугольной области того же размера.

Действительно, в результате численного эксперимента на большом наборе полиномов-кандидатов для факторизации 34-значного числа $n = 31593021658093170959102286152343 77$ показано, что просеивание по особой области дает преимущество перед просеиванием по прямоугольной области. Как характерный результат здесь приведены данные эксперимента, полученные для трех различных m при фиксированном p среднего размера, представляющие собой результаты просеивания массива из 1000 полиномов по особой и прямоугольной областям. Так как использовались полиномы 3-й степени, m выбиралось порядка $\sqrt[3]{n}/p$, по рекомендации Кляйнюнга параметр p состоял из произведения нескольких небольших простых чисел сравнимых с единицей по модулю d, граница факторной базы $B \approx 20000$.

Уточним, как в этом эксперименте определялась высота особой области. Чтобы рост нормы полинома в секторе не превышал роста нормы в прямоугольной области, границу b_s для высоты сектора можно выбрать как $b_s = A/C$, где A – радиус просеивания по прямоугольной области, а $= \max(c, e)$, и где и e —- упоминавшиеся ранее границы основания сектора.

NN	c	e	b_s	Размер области	Найдено гладких	Плотность r_s
0	-10	4	100	70800	512	0,0072
1	-8	3	125	86750	762	0,0088
2	-6	1	167	98363	583	0,0059

Таблица 1: Результаты просеивания по особой области

NN	c	e	b	Размер области	Найдено гладких	Плотность r_p
0	-1000	1000	35	70035	409	0,0058
1	-1000	1000	43	86043	596	0,0069
2	-1000	1000	49	98049	400	0,0041

Таблица 2: Результаты просеивания по прямоугольной области

Очевидно, такое условие является достаточным для того, чтобы норма полинома в секторе, оцениваемая как $b^d M$, не превысила нормы $b^d f(a/b)$, для $a \in [-A; A]$. Затем, для прямоугольной области граница b выбирается таким образом, чтобы площади обеих областей были примерно одинаковыми.

В результате плотность гладких (см. таб. 1 и 2) в особой области оказалась в среднем на 23% выше, чем в прямоугольной. Следующий график наглядно показывает соотношение плотности гладких в секторе (r_s) и прямоугольной области (r_p) для части полиномов из эксперимента с параметрами $m = 276147977$, $p = 13 \cdot 19 \cdot 61 = 15067$.

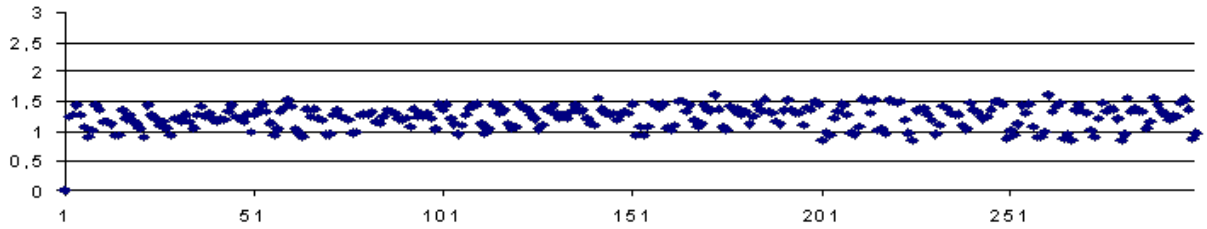


Рис. 5: Отношение доли гладких найденной при просеивании по сектору к доле гладких найденной при просеивании по прямоугольной области того же размера для различных порождающих полиномов в модификации метода Кляйнюнга

Из рис. 5 хорошо видно, что почти все полиномы эффективнее просеивать по сектору, и выигрыш при этом может достигать 50% по сравнению с обычным просеиванием.

В **четвертой главе** описывается структура и состав программного комплекса, использованного для практической апробации методик и получения статистически достоверных оценок, кратко обосновывается необходимость его создания, даются ссылки на программные средства, которые были

использованы помимо специально разработанных для целей диссертационной работы, описывается методика проведенных экспериментов.

Основные проблемы, которые были решены для создания программной системы:

1. Выделение в отдельные логические блоки функций 1) для генерации исходных полиномов просеивания, 2) генерации большого числа их вариаций и детальной теоретической оценки свойств, 3) фактического просеивания по большому набору полиномов и 4) последующего сбора статистики для построения графиков и обоснования теоретических оценок;

2. Реализация в качестве модуля Delphi системы для работы с арифметикой длинных чисел, включая операции в конечных полях $\mathbb{Z}_l$;

3. Реализация обобщенной процедуры просеивания, позволяющей использовать максимально возможное количество памяти компьютера, а также просеивать по особым областям;

4. Оптимизация процедуры просеивания: просеивание "в обратную сторону приближенное вычисление логарифма значений полинома (значительное ускорение по сравнению с тривиальными методами);

5. Оптимизация процедуры поиска факторной базы: реализация алгоритмов Шенкса-Тоннели (для КР) и Нидеррайтера (РЧП) для поиска корней полинома просеивания по модулю $p \in FB$ (значительное ускорение по сравнению с алгоритмами полного перебора);

6. Организация внешних вызовов в систему компьютерной алгебры PARI/GP для тестирования корректности работы программы, а также для сравнения скорости работы реализованных алгоритмов.

Отметим, что, хоть их и не много, существуют свободно доступные готовые реализации таких популярных алгоритмов как квадратичное решето и решето числового поля. Наиболее известные и зарекомендовавшие себя это проекты Msieve[7], GGNFS[8], а также система компьютерной алгебры PARI/GP[9]. Также некоторые из нужных нам алгоритмов реализованы в коммерческом пакете Wolfram Mathematica. Однако для целей, заявленных в диссертационной работе, было необходимо произвести достаточно тонкую настройку и модификацию общего алгоритма, которую невозможно сделать

[7] http://www.boo.net/ jasonp/qs.html

[8] http://www.math.ttu.edu/ cmonico/software/ggnfs/, активная разработка прекращена в 2005

[9] http://pari.math.u-bordeaux.fr/

в существующих готовых программных продуктах. Вместе с тем, полная реализация, например, эффективного алгоритма решета числового поля стояла за рамками данного диссертационного исследования, поскольку сама по себе является неоправданно трудоемкой задачей. В результате был создан программный комплекс, реализующий отдельные этапы алгоритмов квадратичного решета и решета числового поля, который позволяет оценить эффективность предложенных в работе методик, а также эффективность целочисленной факторизации в целом. Акцент в данном случае был сделан на генерацию полиномов, просеивание и подсчет оценок.

Программный комплекс реализован в среде Delphi и состоит из 4-х отдельных, но логические связанных друг с другом программ: для генерации исходного полинома, подходящего для процедуры факторизации; генерация набора его вариаций, вычисление их свойств и подсчет критериев; просеивание, включая просеивание по особой области и по подинтервалам; подсчета статистики для построения графиков и получения обобщенных численных оценок.

Общий объем исходных текстов составляет примерно 5000 строчек кода, из которых около 20% занимает реализация на языке Object Pascal библиотеки для быстрой работы с большими целыми числами. Также были реализованы следующие необходимые для работы алгоритмы теории чисел: алгоритм решения квадратичного уравнения по модуля простого числа Шенкса-Тоннели, алгоритм "поднятия"решения по модулю p^{k+1} при известном решении под модулю p^k (поднятие Гензеля), алгоритм Бернштейна приближенного значения функции Дикмана-де Брюина, алгоритм быстрого поиска корней полинома произвольной степени по модулю произвольного большого простого числа (алгоритм Нидеррайтера). Для оценки корректности реализованных алгоритмов использовалась система компьютерной алгебры PARI/GP.

Были проведены следующие численные эксперименты:

1. эксперимент по оценки сложности метода решета числового поля, ограниченного входными числами $n < 10^5$ и квадратичными полиномами факторизации;

2. эксперимент, оценивающий эффективность просеивания по подинтервалам для n различной длины и различных простых чисел p;

3. эксперимент, оценивающий эффективность просеивания по подинтервалам в модификации КР Занга;

4. эксперимент, оценивающий эффективность просеивания в гибридном методе по особой области — вдоль оптимальной прямой;

5. эксперимент для сравнения просеивания по прямоугольной области с предложенным в диссертации просеиванием по сектору.

В **заключении** приведены основные выводы по диссертации, сформулированы полученные научные и практические результаты, состоящие в следующем:

1. Описана, реализована и проанализирована методика просеивания по подинтервалам в методе факторизации квадратичного решета (КР), которую также можно использовать в методе факторизации числового поля (РЧП), а также в модификации КР Занга. На примере КР видно, что эта стратегия может давать существенный выигрыш, уменьшая величины верхней границы простых чисел в факторной базе и радиуса интервала просеивания, предоставляя дополнительные возможности для параметризации алгоритма, а также допуская его распараллеливание.

2. Описана методика выбора и просеивания по особой области полиномов для алгоритма факторизации числового поля, позволяющая в среднем получать до 20% больший выход гладких по сравнению с обычным просеиванием, а значит быстрее находить лучший полином на первом шаге алгоритма и быстрее находить достаточное количество гладких чисел для факторизации n, чем это возможно в обычном методе РЧП.

3. Разработан программный комплекс, реализующий процедуру просеивания для алгоритмов квадратичного решета и решета числового поля, позволяющий оценивать скорость решения задачи факторизации этими алгоритмами при различных параметрах. Получена численная оценка, подтверждающая эффективность предложенных методик.

Поскольку рассматриваемые алгоритмы квадратичного решета и решета числового поля являются лучшими на сегодняшний день для разложения произвольных больших составных целых на простые множители, это позволяет говорить о том, что с помощью результатов, изложенных в диссертации, можно сделать процедуру факторизации более эффективной.

Список публикаций по теме диссертации

1. В изданиях из списка ВАК:

[1] Зиятдинов Д.Б. *Об одном подходе к проблеме факторизации натуральных чисел* [Текст] / А.А. Бойко , Д.Б. Зиятдинов , Ш.Т. Ишмухаметов // Известия вузов. Математика. — 2011. — №4. — С. 15–22.

[2] Зиятдинов Д.Б. *Об одной стратегии в процедуре просеивания для факторизации больших натуральных чисел* [Текст] / Д.Б. Зиятдинов, Р.Г. Рубцова // Ученые записки Казанского университета. — 2011. — вып. 153. — т. 1. — С. 231–239.

2. Прочие публикации:

[3] Зиятдинов Д.Б. *Об одной оценке метода решета числового поля* / Д.Б. Зиятдинов // Труды VII международной научно-практической конференции «Инфо-коммуникационные технологии глобального информационного общества». — 2009. — Казань. — http://iktgio.mcrt.ru/rusiktgio/tezisy

[4] Зиятдинов Д.Б *Методы защиты информации с открытым ключом и математические проблемы* / Зиятдинов Д.Б., Ишмухаметов Ш.Т. // Материалы ежегодной научно-практическая конференция «Инновации РАН-2010». — 2010. — Казань: Изд-во «Слово». — С. 303.

[5] Зиятдинов Д.Б. *О проблеме выбора полинома в методе решета числового поля* / Д.Б.Зиятдинов, Ш.Т. Ишмухаметов, Р.Г.Рубцова // Труды III Всероссийской конференции "Информационные технологии в системе социально–экономической безопасности России и ее регионов". — 2010. — Казань: Изд-во ТГГПУ. — С. 177–183.

3. Использованные источники

[6] Agrawal M., Kayal N., Saxena N. *PRIMES is in P* // Annals of Mathematics. — 2004. — T. 160. — № 2. — P. 781–793

[7] Bernstein D.J. *Introduction to post-quantum cryptography.* Springer-Verlag Berlin Heidelberg, 2009

[8] Boender H., Riele H. *Factoring Integers with Large-Prime Variations of the Quadratic Sieve*, Centrum voor Wiskunde en Informatica, No. NM-R9513, 1995.

[9] Briggs M. *An Introduction to the General Number Field Sieve* // Master's Thesis, Virginia Polytechnic Institute and State University, Blacksburg, Virginia -1998. — P. 1–84.

[10] Buhler J.P., Lenstra Jr H.W., Pomerance C. *Factoring Integers with the Number Field Sieve* // The Development of the Number Field Sieve, LNM 1554 (1993) P. 50–94.

[11] Buhler J., editor. *Algorithmic Number Theory: Proc. ANTS-III*, Portland, OR, volume 1423 of Lecture Notes in Computer Science. Springer–Verlag, 1998.

[12] Crandall R.E., Pomerance C. *Prime numbers: A Computational Perspective.* Springer, 2002.

[13] Granville A. *Smooth numbers: computational number theory and beyond* // Algorithmic Number Theory MSRI Publications Volume 44, 2008.

[14] Lenstra A.K., Lenstra H.W. Jr., Manasse M.S., Pollard J.M., *Factoring integers with the number field sieve* / in [16] P. 11–42.

[16] Lenstra A., Lenstra H. (Eds) *The Development of the Number Field Sieve* // LNM v.1554, Springer-Verlag, Berlin, 1993.

[17] Kleinjung Th., Aoki K., Franke J., Lenstra A., Thomé E., Bos J., Gaudry P., Kruppa A., Montgomery P., Osvik D. A., te Riele H., Timofeev A., Zimmermann P. *Factorization of a 768-bit RSA modulus.* Online report, 18 Feb 2010.

[18] Kleinjung T. *On Polynomial Selection for the General Number Field Sieve*/ Math. Comp. 75 (2006), P. 2037–2047.

[19] Landquist E. *Possible Ways to Extend Zhang's Special Quadratic Sieve*, 2003.

[20] Murphy B. A. *Polynomial Selection for the Number Field Sieve integer Factorisation Algorithm* // A thesis submitted for the degree of Doctor of Philosophy of The Australian National University, 1999.

[21] Pomerance C. *A Tale of Two Sieves* // Notices of the AMS 43 (12): P. 1473–1485, Dec 1996.

[22] Pomerance C. *Multiplicative independence for random integers* // Analytic Number Theory, vol. 2: Proceedings of a Conference in Honor of Heini Halberstam, Birkhäuser, Boston, 1996.

[23] Pomerance C. *The quadratic sieve factoring algorithm* // Advances in Cryptology, Proceedings of Eurocrypt 84, Paris, 1984.

[24] Rothe J. *Complexity theory and cryptology: an introduction to cryptocomplexity*, Springer Berlin Heidelberg New York, 1998.

[25] Williams C.P., Clearwater S.H. *Ultimate zero and one: computing at the quantum frontier*. Springer-Verlag New York, Oct 1999.

[26] Zhang M. *Factorization of the Numbers of the Form* $\mathbf{m^3 + c_2 m^2 + c_1 m + c_0}$. // in [11], P. 131–136.

[28] Ишмухаметов Ш.Т. *Методы факторизации натуральных чисел.* — Казань: Казан ун.-т., 2011.