МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им М.В.Ломоносова

Механико-математический факультет

Реферат
П.Г. Лежён Дирихле: "Лекции по теории чисел"

Выполнил:

Студент 5 курса 531 группы
Ковальчук А.А.

Преподаватель:

Доцент, к.ф.-м.н.
Смирнова Г.С.

Москва, 2022 г.

Оглавление

Глава 1

Введенеие

Тема моего реферата, как уже можно было понять из названия - книга П.Г. Лежена Дирихле ”Лекции по теории чисел”. По моему мнению, теория чисел - это один из основополагающих разделов математики. Зародившись еще в древнем мире, этот раздел математики смог сохранить свою целостность и сильно спрогрессировать за последние столетия. По своим методам теория чисел делится на четыре части: элементарную, аналитическую, алгебраическую и геометрическую. Сейчас методы теории чисел широко применяются в криптографии, вычислительной математике, информатике.

Лично для меня, теория чисел - это тот раздел, который сочетает в себе элегантность формулировок, красоту свойств и изящные ходы в доказательствах. Помню, как на первом курсе я слушал лекции Н.Г. Мощевитина и не раз удивлялся тому, как даже из понятных обычному человеку вещей можно за полтора часа вывести фундаментальный теоритический базис и сформулировать ряд проблем, которые до сих пор не нашли решение. Особенно мне запомнилась проблема простых чисел-близнецов, так как утверждения, связанные с простыми числами у меня всегда вызывали неподдельный интерес.

Также отмечу, что и сейчас я часто сталкиваюсь с вопросами из области теории чисел, решая уже вычислительные задачи по олимпиадному программированию и не только. Понимание основ теории чисел помогает продумывать алгоритмы с более оптимальной асимптотической сложностью, а также видеть более быстрые ходы там, где обычный человек, интересующийся математикой, не заметил бы.

Надеюсь я смог заинтересовать читателя. Закончить введение я бы хотел словами Аристотеля: "Математика выявляет порядок, симметрию и определённость, а это – важнейшие виды прекрасного". Мне кажется, что именно эти слова точно описывают раздел математики, который сейчас будет рассмотрен. Приступим.

Глава 2

Биография ученого

Иоганн Петер Густав Лежён-Дирихле (нем. Johann Peter Gustav Lejeune Dirichlet) - немецкий математик, внёсший существенный вклад в математический анализ, теорию функций и теорию чисел. Член Берлинской, Петербургской и многих других академий наук.

Дирихле родился 13 февраля 1805г. в вестфальском городе Дюрене в семье почтмейстера. Его предки были выходцами из бельгийского городка Ришле (Richelet), этим обусловлено происхождение необычной для немецкого языка фамилии. Часть фамилии «Лежён» имеет аналогичное происхождение - деда называли «молодым человеком из Ришле» (фр. Le Jeune de Richelet).

2.1 Дество и юность

Дирихле с малых лет увлекался математикой и тратил деньги, которые ему давали на карманные расходны, на покупку учебников по этой науке. В 12 лет он поступил в гимназию в Бонне, в 14 лет - в иезуитский колледж в Кёльне, где он учился у Георга Ома (1789-1854 гг.). К 16 годам Дирихле получил школьное образование и был готов поступать в университет. Он отправился во Францию, привезя с собой работу немецкого математика Гаусса (1777- 1855 гг.). В качестве учителей Дирихле были некоторые из ведущих математиков, и он смог извлечь большую пользу из опыта общения с такими французскими математиками как Фурье (1768-1830 гг.), Франкёром (1773-1849 гг.), Лапласом (1749-1827 гг.), Лакруа (1765- 1843 гг.), Лежандром (1752-1833 гг.) и Пуассоном (1781-1840 гг.). С лета 1823 года Дирихле преподавал немецкий язык жене и детям генерала Максимильена Себастьена Фуа (1775- 1825 гг.), живя в его доме в Париже. В это время начинают появляться первые научные работы Дирихле.

2.2 Статьи, открытия, достижения

В 1825 году Дирихле вместе с Лежандром доказал великую теорему Ферма для частного случая $n = 5$. Теорема утверждала, что для $n > 2$ не существует ненулевых целых чисел x, y, z таких, что $x^n + y^n = z^n$. Случаи $n = 3$ и $n = 4$ были доказаны Эйлером (1707-1783 гг.) и Ферма (1601-1665 гг.).

Доказательство разбивалось на 2 случая. Дирихле доказал случай, когда одно из чисел x, y, z делится на 5 и на 2, и представил свою работу Парижской академии в июле 1825 года. Лежандр был назначен одним из рецензентов, и он смог доказать случай, когда одно из чисел x, y, z делится на 5, а другое из x, y, z делится на 2, завершив доказательство. Полное доказательство было опубликовано в сентябре 1825 года.

После этого Дирихле дал доказательство теоремы Гаусса для биквадратичных остатков. Помимо этого он показал большую роль анализа и теории аналитических функций для решения проблем теории чисел. Известна доказанная им теорема о существовании бесконечно большого числа простых чисел во всякой бесконечной арифметической прогрессии из целых чисел, первый член и разность которой - числа взаимно простые. Дирихле первым дал точное доказательство сходимости рядов Фурье, известное как признак Дирихле, а в вариационном исчислении привел так называемый принцип Дирихле.

В 1827 году юноша по приглашению Александра фон Гумбольдта устроился на должность приват-доцента университета Бреслау (Вроцлав). В 1829 году он перебирается в Берлинский университет, где проработал непрерывно 26 лет, сначала как доцент, затем (с 1831 года) как экстраординарный, а с 1839 года как ординарный профессор Берлинского университета.

В 1855 году Дирихле становится в качестве преемника Гаусса профессором высшей математики в Гёттингенском университете.

Глава 3

Аннотация

Книга П.Г. Лежена Дирихле "Лекции по теории чисел" была составлена его другом, Рихардом Дедекиндом, по лекциям, прочитанным Дирихле в 1856-1857 годах в Гёттингенском университете. Сейчас эта книга считается одним из классических трудов по теории чисел, и она до сих пор не потеряла своей значимости в этой области математики.

Стоит отметить, что на немецком языке книга выдержала четыре издания, на русском языке появилась впервые в 1936 году. Книга состоит из пяти основных глав, а также 10 дополнительных глав: дополнений Дедекинда и приложения - статьи Б.Н. Делоне о геометрии бинарных квадратичных форм. В книге Дирихле дано чисто арифметическое изложение теории квадратичных форм, поэтому дополнительно необходимо изучить статью Делоне, чтобы более глубоко понять смысл важнейших теорем, относящихся к теории квадратичных форм.

Первые три главы книги состоят из теории, которая является классической для элементарных курсов по теории чисел. В этих главах излагаются общие свойства делимости чисел, общая теория сравнений и теория квадратичных вычетов. Две последние главы содержат подробное изложение арифметической теории квадратичных форм.

В этом реферате я хочу более подробно разобрать теорию, которая изложена в первой главе, так как она является основополагающей для изучения последующей теории.

Глава 4

Содержание первой главы

В этой главе разберем краткие выводы, которые читатель может сделать из первой главы, приведем свойства, теоремы и части их доказательств.

4.1 Параграф §1

В первом параграфе строго обосновываются переместительное и сочетательное свойство умножения. Автор указывает на то, что это необходимо, так как именно такие базисные свойства имеют важное значение в теории чисел. Выводы можно сформулировать следующим образом:

1. При умножениии двух целых положительных чисел множимое можно заменить множителем и обратно; по этой причине исчезает различие между названиями "множимое" и "множитель", и они оба называются сомножителями: $ab = ba$

2. В случае трех целых положительных чисел порядок выполнения операции умножения неважен, то есть: $(ca)b = (cb)a = c(ab)$

4.2 Параграф §2

Параграф начинается с замечания о том, что утверждения §1 могут иметь место для любой системы S положительных чисел $a, b, c, ...$ Проводим вычисления следующим образом: берем какие-нибудь два числа, принадлежащие системе S, и составляем их произведение; система чисел S', состоящая из этого произведения и остальных чисел системы S, содержит одним числом меньше, нежели система S.

4.3 Параграф §3

Вводится определения кратного числа. Когда число a есть произведение двух чисел b и m, то a называется кратным b. Из этого определения вытекают следующие положения, которые далее будут часто использоваться, а именно:

1. Если a - кратное b, b - кратное c, то a - кратное c. То есть выполняется свойство транзитивности. Стоит заметить, что если в ряду чисел каждое делится на следующее за ним, то каждое число есть кратное всех последующих чисел.

2. Если числа a и b - кратные числа c, то их сумма и разность тоже кратные числа c.

4.4 Параграф §4

В учении о делимости чисел весьма важное значение имеет следующий вопрос: даны два целых положительных числа a и b; нужно найти общие делители этих чисел, то есть такие числа δ, которые делят одновременно a и b.

В параграфе рассматривается деление с остатком и приводится алгоритм Евклида, который позволяет рекурентно искать наибольший общий делитель двух чисел. Из доказательства этого утверждения следует, что общие делители чисел a и b вполне совпадают с общими делителями некоторого числа h, которое всегда может быть найдено при помощи указанного алгоритма. Это число h называется наибольшим общим делителем чисел a и b.

4.5 Параграф §5

В этом параграфе особое внимание обращается на тот частный случай, когда НОД чисел a и b равен единице. Такие числа называют взаимно простыми. Если a и b - числа взаимно простые, а k - произвольное число, то всякий общий делитель чисел ak и b есть в то же время общий делитель чисел k и b.

Обращается внимание на частные случаи этой теоремы:

1. Если a и k есть числа взаимно простые с b, то и произведение ak есть число взаимно простые с b.

2. Если b, будучи простым относительно a, делит произведение ak, то оно делит и k.

3. Если имеем два ряда таких чисел $a, b, c, d, ...$ и $\alpha, \beta, \gamma, \delta, ...$, что каждое число первого ряда простое относительно каждого числа второго ряда, то произведение $abcd...$ всех чисел первого ряда будет простым относительно произведения $\alpha\beta\gamma\delta...$ всех чисел второго ряда.

4. Если числа a и α взаимно простые, то всякая степень числа а должна быть взаимно простой относительно всякой степени числа α.

4.6 Параграф §6

Если дан ряд чисел $a, b, c, d, ...$, то существует одно и только одно число m, имеющее то свойство, что всякое число, входящее множителем одновременно в $a, b, c, d, ...$, входит также и в m, и обратно, всякий делитель m должен делить все данные числа $a, b, c, d, ...$ Это число m называется общим наибольшим делителем данных чисел. Исключение составляет тот случай, когда все данные числа равны нулю. Ряд чисел называется взаимнопростым, если и только если всякие два из них взаимно простые.

4.7 Параграф §7

В этом параграфе рассматривается вопрос обратный тому, который описан в предыдущем параграфе: дан ряд чисел $a, b, c, d, ...$ и требуется найти все общие кратные данных чисел, т. е. такие числа, которые делятся на каждое из данных чисел. Нетрудно доказать, что все кратные чисел $a, b, c, d, ...$ совпадают с кратным некоторого вполне определенного числа μ, которое называется общим наименьшим кратным данных чисел.

Всякое число, которое делится на каждое из вазимно простых чисел $a, b, c, d, ...$, делится также и на их произведение $abcd...$

4.8 Параграф §8

В этом параграфе формулируется теорема о единственности представления любого составного числа в виде произведения конечного числа простых чисел. Напомним, что составным является число, которое кроме единицы и самого себя делится еще на какое-то значение.

Теорема формулируется следующим образом: всякое составное число всегда может быть прелставлено и притом только одним способом в виде произведения конечного числа простых чисел. Доказательство этой теоремы мы опустим и подметим следующее важное следствие: мы можем разложению составного числа m дать более удобную форму в виде произведения простых чисел в степенях, то есть $m = a^\alpha b^\beta c^\gamma ....$

Стоит отметить, что эта теорема имеет большой вес для решения ряда задач, а также доказательства некоторых утрвеждений. К примеру, зная разложение составного числа в произведение простых в степенях, можно определить количество всех делителей числа m по формуле $(\alpha + 1)(\beta + 1)(\gamma + 1)...$ Это следует из того, что любой делитель числа m есть некоторая комбинация произведения простых чисел, входящих в разложение числа m, в степенях от 0 (что значит, что мы не берем данный делитель) до максимальной.

4.9 Параграф §9

Только что доказанная теорема дает весьма удобный критерий для решения вопроса, делится ли число m на число n, если мы допустим только, что оба числа уже разложены на простые множители. Критерий основан на идеях, которые описаны в предыдущем параграфе, поэтому мы не будем акцентировать на нем внимание. Обоснование можно также найти в книге.

4.10 Параграф §10

В этом параграфе мы возвращаемся к задаче, которая была рассмотрена в 6 параграфе. Она заключается в нахождении общего наибольшего делителя нескольких чисел, предполагая, что эти числа разложены на простые множители.

Из этих последних мы иключаем все те, которые не входят в одно или в несколько данных чисел. Если бы таким образом пришлось исключить все простые множители, тогда общим наибольшим делителем данных чисел являлась бы единица. В противном случае, остается после этого предварительного исключения, например число, которое входит по крайней мере один раз в разложение каждого из данных чисел.

Затем считаем сколько раз это число входит в разложение каждого из этих чисел и получаем значение показателя для данного числа. Подобным образом поступаем со всеми остальными числами и находим значение показателей для них. Этот способ нахождения наибольшего делителя основан на том, что общий наибольший делитель может содержать только те простые множители, которые входят в каждое из данных чисел, и притом каждый их этих множителей входит в общий делитель не чаще, чем каждое из данных чисел. Абсолютно аналогичным образом решается задача о нахождении наибольшего общего кратного нескольких чисел. В состав наименьшего общего кратного должны входить все простые числа, входящие в состав данных чисел, и при том с наибольшими показателями.

4.11 Параграф §11

В этом параграфе нас знакомят с так называемой функцией Эйлера $\varphi(m)$, которая возвращает количество чисел от 1 до m взаимнопростых с m. В параграфе ставится вопрос о нахождении общего выражения для функции $\varphi(m)$. То есть необходимо решить следующую задачу:

Числа $a, b, c...$ являются взаимно простыми и входят в качестве множителей в m. Требуется определить сколько чисел в ряде $1, 2, 3, ..., m$ не будут делиться ни на одно из чисел $a, b, c...$

Опишем кратко алгоритм решения данной задачи. В первую очередь необходимо исключить из ряда, который мы описали выше, все числа, которые делятся на число a: это числа $a, 2a, 3a, ..., \frac{m}{a}a$. Их число равно $\frac{m}{a}$. Если мы исключаем эти числа из ряда, то по понятным причинам остается $m - \frac{m}{a} = m(1 - \frac{1}{a})$ чисел, которые уже не делятся на a. Далее производим аналогичные действия для $b, c, ...$

Итого получим следующий вывод: если $a, b, c, ..., k, l$ - различные простые числа, которые входят в состав m, то количетсво чисел, взаимно простых с m и входящих в ряд $1, 2, ..., m$ определяется формулой:

$$m(1 - \frac{1}{a})(1 - \frac{1}{b})...(1 - \frac{1}{k})(1 - \frac{1}{l})$$

4.12 Параграф §12

Из утверждения, доказанного в предыдущем параграфе, формулируется следующая теорема: Если m и m' взаимно простые, то $\varphi(mm') = \varphi(m)\varphi(m')$. Это свойство называется мультипликативным свойствоv функции и несет в себе важное значение для ряда вычислительных задач. Также стоит отметить, что теорема верна для произведения любого числа множителей в случае, если они попарно взаимно просты.

4.13 Параграф §13

Вопрос об определении функции $\varphi(m)$ представляет собой частный случай следующей задачи: дан ряд чисел $1, 2, 3, ..., m$ и требуется найти число тех чисел этого ряда, которые имеют общим наибольшим делителем с m число δ, причем δ есть один из делителей числа $m = n\delta$. Опишем доказательство, так как оно компактно и хорошо показывает применение предыдущих умозаключений.

Сведем эту задачу к предыдущей: очевидно, что все искомые числа находятся между числами $\delta, 2\delta, 3\delta, ..., n\delta$. Для того, чтобы δ было наибольшим общим делителем числа $m = n\delta$ и какого-нибудь числа вида $r\delta$, необходимо и достаточно, чтобы r и n были числами взаимно простыми. Следовательно, искомых чисел столько, сколько найдется чисел ряда $1, 2, 3, ..., n$, взаимно простых с n. Число таких чисел равно $\varphi(n)$. Когда $\delta = 1$, приходим к частному случаю, рассмотренному в предыдущем параграфе. Закончим тем, что приведем еще одно свойство функции $\varphi(m)$. Если n пробегает значения всех делителей числа m, то имеет место следующее равенство:

$$\sum_n \varphi(n) = m$$

4.14 Параграф §14

Приведенное выше доказательство этого важного свойства функции $\varphi(m)$ получается непосредственно из определения и не требует предварительного определения вида самой функции. Дополнительно отмечу, что в в этом параграфе рассматривается другое доказательство этого же факта при помощи уже известного нам выражения для функции $\varphi(m)$. Не будем долго на этом останавливаться.

4.15 Параграф §15

Этот параграф посвящен изучению проблемы определения показателя наивысшей степени простого числа p, входящей множителем в факториал $m!$, где m - некоторое целое число. Пусть m' - наибольшее целое число, содержащееся в дроби $\frac{m}{p}$. Тогда из числа m сомножителей произведения $m!$ на p делятся следующие m' сомножителей: $p, 2p, ..., m'p$. Искомый показатель равен показателю наивысшей степени числа p, входящей в произведение $1 * 2 * 3 * ... * m' * p^{m'}$. Он равен сумме m' и показателя наивысшей степени p, входящей в произведение $m!$. Тогда имеем, что искомый показатель равен $m' + m'' + m''' + ...$, где $m'', m''', ...$ - наибольшие целые числа, которые содержатся в дробях $\frac{m'}{p}$, $\frac{m''}{p}$ и т. д.

Анализируя информацию выше, можно прийти к следующей теореме: если $m = f + g + h + ...$, то отношение $\frac{m!}{f! * g! * h! ...}$ является целым числом. Эту теорему также оставим без доказательства.

4.16 Параграф §16

В этом параграфе автор делает подытог. Он обращает внимание на то, что большая часть описанных утверждений и теорем строится на основе алгоритма нахождения наибольшего общего делителя. В параграфе приводится пример целых комплексных чисел и показывается, как теория, описанная в этой главе для обыкновенных целых чисел, может быть расширена на целые комплексные.

Глава 5

Заключение

Подводя итог всему выше написанному, я хочу заметить, что Дирихле сделал огромный вклад в науку не только как ученый и математик, но и как преподаватель. Последователями Дирихле стал целый ряд учёных. Среди них такие известные немецкие математики, как Фердинанд Эйзенштейн, Леопольд Кронекер, Рудольф Липшиц и многие другие. Многочисленность учеников и их плодотворная научная деятельность наглядно доказывает, что труды Лежёна Дирихле действительно были очень значимыми и внесли огромный вклад в науку Германии.

Дирихле прожил не самую долгую жизнь: он скончался в возрасте пятидесяти четырех лет. Его столь ранний уход из жизни был связан с тем, что он всю свою жизнь посвятил науке, при этом не отдавая должного внимания своему здоровью. Болезни дали о себе знать и стали причиной его смерти.

Меня всегда впечатляли такие личности, ведь открытия, которые делают и делали ученые напрямую связаны с личностными качествами. Составляя этот реферат, я освежил часть знаний, которые были усвоены мной на начальных курсах механико-математического факультета МГУ, а также узнал много интересного об этом ученом. Надеюсь, что читатель также найдет этот реферат полезным для себя, и, самое главное, вдохновиться на дальнейшее изучение математики.

Глава 6

Список используемых ресурсов

[1] Лежен Дирихле П. Г., Лекции по теории чисел. В обработке и с добавлениями Р. Дедекинда. Перевод с немецкого А. И. и С. И. Каменецких под редакцией проф. Б. И. Сегала, с приложением статьи проф. Б. Н. Делоне „Геометрия бинарных квадратичных форм". М.-Л., ОНТИ, Главная редакция общетехнической литературы, 1936, 403 стр.

[2] Дирихле, Петер Густав Лежён, Биография, Научная деятельность `https://ru.wikipedia.org`