ОБЗОРНАЯ ЛЕКЦИЯ ПО ТЕОРИИ ЧИСЕЛ

1 Вводные сведения, касающиеся алгебраических чисел

Число $\alpha \in \mathbb{C}$ называется алгебраическим, если существует ненулевой многочлен $f(x) \in \mathbb{Z}[x]$ такой, что $f(\alpha) = 0$. Многочлен наименьшей степени, для которого $f(\alpha) = 0$, называется минимальным многочленом числа α. Минимальный многочлен определяется однозначно с точностью до умножения на целую постоянную. Степень числа α это степень минимального многочлена. Число α называется целым алгебраическим, если старший коэффициент минимального многочлена равен 1. Если число α не является алгебраическим, то оно называется трансцендентным. Множество алгебраических чисел образует поле.

Пример 1. Рациональное число $q \notin Z$ является алгебраическим первой степени, но не является целым алгебраическим. Число $\sqrt{2}$ является целым алгебраическим степени 2.

Существование трансцендентных чисел вытекает из счетности множества алгебраических чисел и несчетности множества комплексных чисел.

Впервые трансцендентное число в явном виде было построено Лиувиллем во второй половине 19 века, это число $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$. Метод Лиувилля позволил доказать трансцендентность чисел π, e.

Д. Гильберт в 1900 г. на Международном математическом конгрессе представил список из 23 открытых проблем, охватывающих все основные разделы математики. К настоящему времени 12 из них признаны полностью решенными, 7 решены частично, 3 признаны слишком расплывчатыми и требующими уточнения и 1 не решена даже частично. В 7-й проблеме Гильберт спрашивает, является ли число $2^{\sqrt{2}}$ трансцендентным. Советский математик А. Гельфонд доказал теорему, которая гласит, что для любого алгебраического числа α, отличного от 0 и 1, и любого алгебраического иррационального числа β число α^{β} является трасн-цендентным. Тем самым, дав утвердительный ответ на 7-ю проблему Гильберта. К примеру, из теоремы Гельфонда и тождества $e^{\pi i} = -1$ немедленно можно вывести трансцендентность числа e^{π}. Несмотря на то, что в работах Лиувилля, Гельфонда и их последователей были развиты мощные аналитические методы доказательства трансцендентности, задача доказательства трансцендентности в общем виде остается крайне трудной. К примеру, до сих пор неизвестно, являются ли числа π^e, π^{π}, e^e, $\ln(\pi)$ трансцендентными (и даже иррациональными).

2 От Великой теоремы Ферма к abc-гипотезе

В 1637 г. П. Ферма оставил на полях одной из книг Диофанта, где рассматривалось уравнение $x^2 + y^2 = z^2$, следующую фразу: "Вместе с тем невозможно разложить куб на два куба или биквадрат на два биквадрата и вообще невозможно разложить никакую степень, большую чем два, на две степени с таким же показателем. Я нашел поистине удивительное доказательство, но поля книги слишком узки, чтобы вместить его".

Великая теорема Ферма. Для любого натурального $n \geq 3$ уравнение $x^n + y^n = z^n$ не имеет решений в натуральных числах.

2.1 Этапы доказательства Великой теоремы Ферма

Историки математики полагают, что Ферма имел ввиду метод бесконечного спуска, который, действительно, позволяет доказать теорему для $n = 4$. И это единственный показатель, для которого теорему удалось доказать средствами элементарной арифметики.

Уже случай $n = 3$ требует привлечения арифметики квадратичного кольца $\mathbb{Z}[\sqrt{-3}]$ и был полностью обоснован Эйлером (1768 г.) более 100 лет после того, как Ферма оставил

свою знаменитую запись. Спустя более 50 лет после этого Дирихле и Лежандр (1825 г.) смогли доказать теорему для $n = 5$. В 1839 г. Ламе доказал теорему для $n = 7$. Практически сразу же после этого Ламе и Куммер независимо предложили доказательство теоремы в общем случае, но оба опирались на необоснованный факт, что числа вида $\sum_{i=0}^{n-2} a_i\zeta^i$, где $a_i \in \mathbb{Z}$, ζ – первообразный корень степени n из единицы, разлагаются единственным образом в произведение простых чисел. Впоследствии оказалось, что это утверждение не только не обосновано, но и неверно. Тем не менее работы Ламе и Куммера позволили выделить целые семейства простых показателей n, для которых верна теорема Ферма.

Последующий прорыв случился лишь в середине 20 века, когда японские математики Шимура и Танияма выдвинули гипотезу о том, что каждой эллиптической кривой $y^2 = x^3+ax^2+bx+c$ соответствует некоторая модулярная функция (т.е. комплексная функция $f : \mathbb{C} \to \mathbb{C}$, инвариантная относительно модулярной группы дробно-линейных преобразований, т.е. $f(\frac{az+b}{cz+d}) = f(z)$, $ad - bc = 1$) (т.е. совпадают их разложения в ряд).

В 1984 г. Г. Фраю удалось свести уравнение Ферма к уравнению эллиптической кривой специального вида, причем этой гипотетической эллиптической кривой нельзя поставить в соответствие ни одну модулярную форму. Тем самым проблема Ферма представляет частный случай гипотезы Шимуры-Таниямы. Окончательное доказательство гипотезы Шимуры-Таниямы было представлено английским математиком Э. Уайлсом в 1995 г. спустя 8 лет непрерывной работы над её доказательством. Стоит отметить, что в 2016 г. Уайлс получил премию Абеля за доказательство Великой теоремы Ферма.

2.2 Обобщение теоремы Ферма для рациональных показателей

Теорема. Уравнение $x^{m/n}+y^{m/n} = z^{m/n}$ не имеет решений в натуральных числах x, y, z при $m \geq 3$, $(m, n) = 1$.

Идеи доказательства.

Исходя из однородности уравнения, достаточно доказать теорему для попарно взаимно простых x, y, z.

Утверждение 1. Если числа α^n, $(\alpha + 1)^n$ являются рациональными для действительного $\alpha > 0$ и натурального n, то число α является рациональным.

Рассмотрим минимальный многочлен $f(x)$ числа α. Он делит аннулирующие многочлены $g(x) = x^n - \alpha^n$, $h(x) = (x + 1)^n - (\alpha + 1)^n$. Из элементарных геометрических соображений вытекает, что многочлены, имеющие общий действительный корень α, не могут иметь общего корня $\lambda \in \mathbb{C}$, отличного от α. Кроме того, α не может быть кратным корнем многочлена $g(x)$, поэтому $f(x) = x - \alpha$, т.е. $\deg(\alpha) = 1$.

Из утверждения 1 вытекает следующее

Утверждение 2. Все решения уравнения при $m = 1$ имеют вид: $x = a^n$, $y = b^n$, $z = (a+b)^n$.

Из этого утверждения вытекает, что $x^m = a^n$, $y^m = b^n$, $z^m = (a+b)^n$. Теперь из взаимной простоты m, n получаем, что $a = \alpha^m$, $b = \beta^m$, $a+b = \gamma^m$. Т.е. $\alpha^m+\beta^m = \gamma^m$, что противоречит Великой теореме Ферма.

Открытая проблема. Существует ли положительное алгебраическое число α, отличное от $1/n$, $2/n$, такое что уравнение $x^\alpha + y^\alpha = z^\alpha$ разрешимо в натуральных числах?

2.3 abc-гипотеза и её следствия

Радикал $R(n)$ натурального числа n это произведение всех различных простых делителей числа n.

В 1985 г. Массер и Остерле выдвинули следующую гипотезу.

abc-гипотеза. Для любого $\varepsilon > 0$ существует постоянная $\kappa(\varepsilon)$ такая, что для любой тройки попарно взаимно простых натуральных чисел a, b, c, таких, что $a+b = c$, выполняется неравенство $c < \kappa(\varepsilon)(R(abc))^{1+\varepsilon}$.

Наиболее сильный доказанный результат (Stewart, Kunrui, 2001) гласит, что

$$\log c \leq \kappa(\varepsilon)(R(abc))^{1/3+\varepsilon},$$

где постоянную $\kappa(\varepsilon)$ можно вычислить в явном виде.

Пример 2. Справедливость *abc*-гипотезы позволила бы получить простое доказательство Великой теоремы Ферма. Действительно, $z^n < \kappa(\varepsilon)(xyz)^{1+\varepsilon} < \kappa(\varepsilon)z^{3+3\varepsilon}$. Т.е. при $n \geq 4$ получаем оценку сверху z и, следовательно, на z^n, универсальной постоянной. Тем самым, теорема Ферма сводилась бы к перебору конечного числа вариантов (хотя, возможно, очень большого).

Пример 3. Результат Stewart-Kunrui позволяет получить оценку сверху для решений уравнения $a^x + b^y = c^z$ с постоянными a, b, c и тем самым свести решение к конечному перебору. Действительно, $z \log c \leq \kappa(\varepsilon)(R(abc))^{1/3+\varepsilon}$, что означает ограниченность сверху переменной z.

3 RSA-криптосистема

В 1940 г. известный американский математик Г. Харди высказал мысль о том, что настоящая первоклассная математика (т.е. чистая теоретическая) в основном бесполезна. И добавил, что это вовсе неплохо, указав, что никто не открыл ни одного применения теории чисел в военных целях. Однако это мнение оказалось ошибочным. Наиболее значительные применения теории чисел были получены как раз в связи с необходимостью секретной передачи информации в военных целях. Пик развития криптографических приложений теории чисел приходится на 70-90-е годы 20 века. С одной стороны, это было вызвано бурным развитием вычислительной техники, а с другой стороны открытием нового направления в криптографии - создание криптосистем с открытым ключом.

Долгое время полагалось, что в любой криптосистеме пользователь, знающий ключ шифрования может легко восстановить и ключ дешифрования. Поэтому оба ключа держались в секрете. Но такой подход имеет существенный недостаток: число ключей в системе растет пропорционально квадрату числа пользователей.

В 1977 г. Ривест, Шамир, Адльманн построили первый пример криптосистемы с открытым ключом (т.е. позволяющей не скрывать ключ шифрования), которая получила название RSA-криптосистемы и является одной из наиболее востребованных и по сей день ввиду её простоты и надежности. Рассмотрим алгоритм RSA-криптосистемы.

Предположим, что пользователь A желает организовать прием секретных сообщений. Для этого пользователь A выбирает два больших различных простых числа p, q, вычисляет $N = pq$, затем выбирает случайное натуральное число e, взаимно простое с $\varphi(N)$ и находит натуральное число d такое, что $ed \equiv 1 (\mathrm{mod}\ N)$. Число N – модуль пользователя A, и число e – открытый ключ пользователя A, публикуются в открытом доступе. Любой пользователь, который желает передать пользователю A секретное сообщение m, вычисляет вычет $y = m^e (\mathrm{mod}\ N)$ и передает его по открытому каналу связи. Пользователь A восстанавливает сообщение m с помощью своего секретного ключа d, т.е. $y^d = m (\mathrm{mod}\ N)$. Для больших p, q вероятность того, что числа m, N окажутся взаимно простыми, близка к 1 и в этом случае корректность протокола обеспечивается теоремой Эйлера. Впрочем, алгоритм корректно работает и в случае нарушения взаимной простоты m, N. В этом случае для обоснования нужно применить малую теорему Ферма по модулям p, q, а затем китайскую теорему об остатках.

Отметим, что стойкость RSA-криптосистемы основана на сложности вычисления $\varphi(N)$ при неизвестных p, q, что в свою очередь связано со сложностью факторизации большого натурального числа.

3.1 Проверка чисел на простоту, генерация больших простых чисел, связь с гипотезой Римана

Для обеспечения стойкости криптосистемы RSA необходимо иметь эффективные алгоритмы генерации больших простых чисел.

Несмотря на то, что известны явные формулы, описывающие множество простых чисел, к примеру, следующая формула Серпинского

$$p_n = [10^{2^n}\alpha] - 10^{2^{n-1}}[10^{2^{n-1}}\alpha],\ \alpha = \sum_{i=1}^{\infty} p_i 10^{-2^i},$$

а также асимптотические формулы $p_n = \theta(n \ln n)$, $\pi(n) \sim n/\ln n$ при $n \to \infty$, эти результаты не применимы для построения больших простых чисел.

Наиболее эффективные алгоритмы построения больших простых чисел созданы для чисел Мерсенна $M_n = 2^n - 1$, для которых известен простой критерий Люка-Лемера: число M_n, $n \geq 3$, является простым тогда и только тогда, когда n простое и $L_n \equiv 0 (\mathrm{mod}\ M_n)$, где $L_0 = 4$, $L_{k+1} = L_k^2 - 2 (\mathrm{mod}\ M_n)$. Эффективность теста Люка-Лемера объясняется двумя причинами: числа Мерсенна легко генерировать, т.к. они состоят из одних единиц в двоичной записи, а проверка условий критерия Люка-Лемера требует полиномиального по n числа двоичных операций. Самое большое известное простое числа - число Мерсенна, состоящее из более 22 миллионов десятичных цифр, было найдено в январе 2016 г. Вместе с тем, неизвестно, бесконечно ли множество простых чисел Мерсенна.

Известны вероятностные алгоритмы проверки числа N на простоту, позволяющие доказывать, что число N составное с вероятностью не меньше $\alpha > 0$ за полиномиальное относительно длины числа N время. Один из таких тестов основан на проверке малой теоремы Ферма $a^{N-1} \equiv 1 (\mathrm{mod}\ N)$ для случайно выбранного a. Очевидно, что в случае невыполнимости данного сравнения можно утверждать, что число N составное. Все известные детерминированные алгоритмы полиномиальной по $\log N$ сложности опираются на модификацию следующей гипотезы Римана: "все нули дзета-функции $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, расположенные в полосе $0 \leq Re(s) \leq 1$ лежат на прямой $Re(s) = \frac{1}{2}$." Отметим, что гипотеза Римана является одной из семи математических задач тысячелетия (решена только одна из них - доказана гипотеза Пуанкаре).

3.2 Задача факторизации и связь с RSA

Как отмечалось, стойкость криптосистемы RSA напрямую зависит от сложности задачи факторизации выбранного модуля N. Многие классические и современные методы факторизации основаны на следующей простой идее.

Пусть $N = ab$, где a, b нечетные числа, тогда $N = t^2 - s^2$, где $t = \frac{a+b}{2}$, $s = \frac{a-b}{2}$. Если числа a, b близки друг к другу, то их можно быстро найти, перебирая значения $t = [\sqrt{N}] + k$, $k = 1, 2, \ldots$, пока не найдем такое t, что число $t^2 - N$ является полным квадратом. Отсюда, в частности, вытекает ограничение на выбор p, q в RSA-криптосистеме: $|p - q|$ должно быть достаточно велико.

Модификация этой идеи состоит в нахождении сравнений вида $t^2 \equiv s^2 (\mathrm{mod}\ N)$ при $t \not\equiv \pm s (\mathrm{mod}\ N)$. В этом случае $(t \pm s, N)$ является нетривиальным делителем числа N. Большинство современных методов факторизации основаны на этой идее и представляют эффективные методы построения таких соотношений $t^2 \equiv s^2 (\mathrm{mod}\ N)$.

Известны специальные методы, которые эффективно находят факторизацию $N = pq$, если $p \pm 1$, $q \pm 1$ имеют небольшие простые делители, что в свою очередь накладывает новые ограничения на выбор параметров RSA-криптосистемы.

Отметим, что наиболее быстрые методы факторизации чисел общего вида имеют субэкспоненциальную сложность относительно $n = \log N$, т.е. $O(\exp(n^\alpha))$, где $0 < \alpha < 1$, что обеспечивает стойкость RSA-криптосистемы при должном выборе параметров. Наиболее быстрые методы факторизации связаны с переходом от целочисленной факторизации к факторизации в кольцах, порожденных присоединением определенных алгебраических элементов.

3.3 Обобщения RSA-криптосистемы

Опишем общую идею того, как можно построить аналог RSA-криптосистемы на более широких множествах, чем целые числа.

На комплексной плоскости рассмотрим множество точек с целыми действительными и мнимыми частями - кольцо гауссовых чисел $\mathbb{Z}[i]$. Эти точки образуют квадратную решетку на комплексной плоскости и с алгебраической точки зрения образуются присоединением элемента $i = \sqrt{-1}$ к полю рациональных чисел $\mathbb{Q}$ и сужением полученного множества до множества целых алгебраических чисел. Кольцо $\mathbb{Z}[i]$ обладает многими свойствами кольца целых чисел: имеет место основная теорема арифметики о единственности разложения в произведение простых, вводится алгоритм Евклида для нахождения НОД.

Убедимся, что в кольце гауссовых чисел имеет место аналог теоремы Эйлера. Алгебраически обосновать теорему Эйлера можно сформулировать так: поскольку порядок элемента a в мультипликативной группе вычетов по модулю N делит порядок самой группы (следствие теоремы Лагранжа), который равен $\varphi(N)$, то $a^{\varphi(N)}$ дает единичный элемент группы. Очевидно, что здесь никак не используется специфика целых чисел, и это же рассуждение можно применить для кольца гауссовых чисел.

Отметим, что $\varphi(N) = (\mathrm{Nm}(p) - 1)(\mathrm{Nm}(q) - 1)$, где $\mathrm{Nm}(a) = |a|^2$.

В дальнейшем мы покажем, что аналог RSA можно ввести в любых квадратичных кольцах (полученных присоединение алгебраического элемента степени 2 к полю рациональных чисел), в которых выполнена основная теорема арифметики о единственности разложения в произведение простых. Мы покажем, что такие аналоги обладают привычными свойствами целочисленной RSA, но при этом позволяют использовать более широкое пространство исходных сообщений без увеличения длины ключей.

Наряду с самой криптосистемой, мы детально исследовали смежные задачи, связанные с генерацией ключей и стойкостью. В частности, нам удалось получить новые критерии простых чисел в квадратичных кольцах, на основе которых мы создали эффективные алгоритмы тестирования на простоту. Детали мы будем подробно рассматривать в нашем курсе.

4 Экстремальные свойства алгоритма Евклида

4.1 Теоремы Кронекера-Валена и Ламе

Хорошо известен факт, что максимум числа шагов для алгоритма Евклида, примененного к двум числам, не превосходящим N, достигается на двух наибольших числах Фибоначчи из отрезка $[1, N]$. Отсюда и из приближенной формулы $f_n \approx \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n$ вытекает, что число шагов алгоритма Евклида есть величина $O(\log N)$ (теорема Ламе).

Рассматривая целочисленные остатки (наименьшие по абсолютной величине) вместо натуральных, можно ускорить алгоритм Евклида. Кронекер и Вален независимо доказали, что выбор наименьших по абсолютной величине остатков на каждом шаге алгоритма Евклида приводит к кратчайшей версии алгоритма Евклида (тот случай, когда жадный алгоритм оказывается оптимальным).

4.2 Аналоги в кольце многочленов

Для кольца многочленов $\mathbb{R}[x]$ определим норму как степень многочлена. Рассматривая последовательность многочленов $f_{n+2}(x) = xf_{n+1}(x) + f_n(x)$, $f_1(x) = 1$, $f_2(x) = x$, видим, что алгоритм Евклида для нахождения НОД $f_{n+1}(x)$, $f_n(x)$ требует n шагов. Иными словами, аналог теоремы Ламе в этом кольце не имеет места.

Тем не менее, теорема Кронекера-Валена остается верной в кольце $\mathbb{R}[x]$.

4.3 Аналоги в квадратичных кольцах

Для квадратичного кольца (евклидового) $\mathbb{Z}[\sqrt{d}]$ определим норму числа $a+b\sqrt{d}$ как величину $|a^2 - b^2 d|$.

Роллетчек доказал удивительный результат: теорема Кронекера-Валена выполняется в $\mathbb{Z}[\sqrt{d}]$ тогда и только тогда, когда $d \neq -11$.

Нам удалось отделить общие (структурные алгебраические) свойства евклидовых колец от свойств элементов данного кольца, которые играют существенную роль в доказательстве теоремы Кронекера-Валена и тем самым мы получили алгоритмы автоматического доказательства этой теоремы в конкретных кольцах. В дальнейшем курсе мы детально обсудим эти свойства, алгоритмы и перспективы их компьютерной реализации.

5 Заключение

Таким образом, алгебраические методы в теории чисел позволяют, с одной стороны, перенести многие результаты, относящиеся к теории натуральных чисел, на более широкие числовые структуры. Для ряда задач элементарной теории чисел именно переход к алгебраическим расширениям позволяет найти исчерпывающее решение, как в случае Великой теоремы Ферма, либо строить рекордно быстрые алгоритмы решения вычислительно сложных задач, таких как факторизация больших натуральных чисел. Вместе с тем, мы видим, что во многих случаях ключевую роль играет и природа самих чисел, а не только их стуктурные свойства, это хорошо иллюстрируется в теоремах Люка-Лемера, Ламе, Кронекера-Валена. Тем самым, теория чисел, имея очень тесные связи с алгеброй, остаётся полноценной и самостоятельной отраслью математики.