

Е. Золотарев

**Теория целых комплексных чисел с
приложением к интегральному исчислению**

**Москва
«Книга по Требованию»**

УДК 51
ББК 22.1
Е11

Е11 **Е. Золотарев**
Теория целых комплексных чисел с приложением к интегральному исчислению / Е. Золотарев – М.: Книга по Требованию, 2021. – 184 с.

ISBN 978-5-458-57028-2

ISBN 978-5-458-57028-2

© Издание на русском языке, оформление
«YOYO Media», 2021
© Издание на русском языке, оцифровка,
«Книга по Требованию», 2021

Эта книга является репринтом оригинала, который мы создали специально для Вас, используя запатентованные технологии производства репринтных книг и печати по требованию.

Сначала мы отсканировали каждую страницу оригинала этой редкой книги на профессиональном оборудовании. Затем с помощью специально разработанных программ мы произвели очистку изображения от пятен, клякс, перегибов и попытались отбелить и выровнять каждую страницу книги. К сожалению, некоторые страницы нельзя вернуть в изначальное состояние, и если их было трудно читать в оригинале, то даже при цифровой реставрации их невозможно улучшить.

Разумеется, автоматизированная программная обработка репринтных книг – не самое лучшее решение для восстановления текста в его первоизданном виде, однако, наша цель – вернуть читателю точную копию книги, которой может быть несколько веков.

Поэтому мы предупреждаем о возможных погрешностях восстановленного репринтного издания. В издании могут отсутствовать одна или несколько страниц текста, могут встретиться невыводимые пятна и кляксы, надписи на полях или подчеркивания в тексте, нечитаемые фрагменты текста или загибы страниц. Покупать или не покупать подобные издания – решать Вам, мы же делаем все возможное, чтобы редкие и ценные книги, еще недавно утраченные и несправедливо забытые, вновь стали доступными для всех читателей.

Въ IV-й главѣ я прилагаю теорію комплексныхъ чиселъ къ одному вопросу интегральнаго исчисленія. Этотъ вопросъ состоитъ въ томъ, чтобы узнать при помощи конечнаго числа дѣйствій интегрируется ли дифференціалъ одного опредѣленнаго вида въ логарифмахъ и поэтому относится къ той части интегральнаго исчисленія, которая обогащена изслѣдованіями Абеля, Лувилля, Чебышева, Вейерштрасса и друг. Я особенно цѣню это приложеніе теоріи комплексныхъ чиселъ, потому что оно выражаетъ новую связь между интегральнымъ исчисленіемъ и теоріею чиселъ.

Е. З.

ОГЛАВЛЕНИЕ.

Глава I.

О функциональных сравненияхъ.

1. Опреѣленіе функциональных сравненій.
2. Дѣлимость одной функціи на другую по нѣкоторому простому модулю.
3. Объ общемъ наибольшемъ дѣлителѣ двухъ функцій по нѣкоторому простому модулю.
4. Одна теорема относительно двухъ функцій взаимно простыхъ по нѣкоторому простому модулю.
5. О дѣлимости произведенія двухъ функцій по нѣкоторому простому модулю.
6. О простыхъ функціяхъ по нѣкоторому простому модулю.
7. О разложеніи функцій на простые множители по нѣкоторому простому модулю.
8. Отдѣленіе кратныхъ множителей.
9. О сравненіяхъ по нѣкоторому простому модулю и нѣкоторой простой функціи.
10. Теорема относящаяся къ такимъ сравненіямъ.
11. Теорема аналогичная теоремѣ Фермата.
12. Другая теорема, дополняющая предыдущую.
13. О числѣ простыхъ функцій данной степени по нѣкоторому простому модулю.
14. Дополненіе относительно разложенія функцій на простые множители по нѣкоторому простому модулю.
15. О функціи $\frac{x^n - 1}{x - 1}$.
16. О періодахъ.
17. Разложеніе функцій $\frac{x^n - 1}{x - 1}$ на простые множители по нѣкоторому простому модулю, при n простымъ.
18. Примѣръ.

Глава II.

О комплексныхъ единицахъ.

19. Общія замѣчанія о комплексныхъ числахъ.
20. Сопряженные комплексныя числа. Норма комплексныхъ чиселъ. Союзное комплексное число.
21. О дѣйствіяхъ надъ комплексными числами.
22. Опреѣленіе комплексныхъ единицъ.
23. Лемма относительно линейныхъ функцій, зависящихъ отъ цѣлыхъ чиселъ.
24. Другая лемма относительно линейныхъ функцій.
25. Объ уравненіи $N_{\mathbb{Q}}x = 1$; особенныя рѣшенія этого уравненія.
26. Объ уравненіи $N_{\mathbb{Q}}x = T$.
27. Приложеніе теоремы, доказанной въ предыдущемъ n° , къ рѣшенію уравненія $N_{\mathbb{Q}}x = 1$.

1°

31. Опредѣленіе независимыхъ рѣшеній.
32. Доказательство существованія системы, состоящей изъ $h - 1$ независимыхъ рѣшеній уравненія $N_r x = 1$.
34. Различныя теоремы, относящіяся къ этой системѣ рѣшеній.
35. Объ основныхъ рѣшеніяхъ уравненія $N_r x = T$.
36. Общее выраженіе всѣхъ основныхъ рѣшеній.
37. Рѣшенія уравненія $N_r x = r$.
38. Общая формула для комплексныхъ единицъ.

Глава III.

Идеальные множители комплексныхъ чиселъ.

39. Краткія историческія замѣчанія о комплексныхъ числахъ.
40. О дѣлимости произведенія нѣсколькихъ комплексныхъ чиселъ на обыкновенное простое число.
42. О дѣлимости нормы комплекснаго числа на обыкновенное простое число.
43. Замѣчанія объ основномъ уравненіи $F(x) = 0$.
44. Постановка главнаго вопроса, рѣшеніе котораго содержится въ этой главѣ.
45. Классификація комплексныхъ чиселъ на простые и сложные.
46. Опредѣленіе степени кратности простаго идеальнаго множителя существующаго комплекснаго числа.
49. Теоремы относительно идеальныхъ чиселъ.
50. Свойство нормы комплексныхъ чиселъ.
53. Разложеніе комплексныхъ чиселъ на простые идеальные множители.
55. Частные случаи комплексныхъ чиселъ.
60. Распределеніе идеальныхъ комплексныхъ чиселъ на классы.

Глава IV.

Приложеніе теоріи комплексныхъ чиселъ къ одному вопросу интегральнаго ис-

61. Постановка вопроса и нѣкоторыя историческія замѣчанія объ интегрированіи алгебраическихъ дифференціаловъ въ логарифмахъ.
64. Приведеніе дифференціала $\frac{(x + A) dx}{\sqrt{x^4 + \gamma x^3 + \delta x^2 + \varepsilon x + \zeta}}$ къ виду $\frac{(x + A) dx}{\sqrt{x(x - 1)(x - \alpha)(x - \beta)}}$.
65. Выраженіе $\int_0^x \frac{(x + A) dx}{\sqrt{x(x - 1)(x - \alpha)(x - \beta)}}$ въ эллиптическихъ функціяхъ.
66. Примѣненіе преобразованія н° 63 къ дифференціалу $\frac{(x + A) dx}{\sqrt{x(x - 1)(x - \alpha)(x - \beta)}}$.
67. Тоже преобразованіе въ эллиптическихъ функціяхъ.
68. Примѣненіе къ дифференціалу $\frac{(x + A) dx}{\sqrt{x(x - 1)(x - \alpha)(x - \beta)}}$ преобразованія н° 64.
69. Тоже преобразованіе въ эллиптическихъ функціяхъ.
70. Условіе интегрируемости дифференціала $\frac{(x + A) dx}{\sqrt{x(x - 1)(x - \alpha)(x - \beta)}}$ въ логарифмахъ.
71. Объ уравненіи $F(\alpha, \beta) = 0$ между параметрами α и β .
72. Другой видъ условій интегрируемости

VI.

nn°

73. Условіе между параметрами α и β , когда P функція четной степени.

74. Три различные случая при рѣшеніи вопроса объ интегрированіи дифференціала $\frac{(x + A) dx}{\sqrt{x(x-1)(x-\alpha)(x-\beta)}}$
въ логарифмахъ и изслѣдованіе первыхъ двухъ случаевъ.

75. Выраженіе параметровъ α и β раціональными функціями одного параметра.

76 — 82 Рѣшеніе задачи въ третьемъ случаѣ.

83. Примѣры.

84 — 88. Прибавленіе.

ГЛАВА I.

0 функціональныхъ сравненійхъ¹.

1.

Пусть A и B будутъ двѣ функціи переменной x вида

$$\begin{aligned} a_0 + a_1x + a_2x^2 + \dots + a_mx^m \\ b_0 + b_1x + b_2x^2 + \dots + b_nx^n, \end{aligned}$$

гдѣ коэффициенты

$$\begin{aligned} a_0, a_1, a_2, \dots, a_m \\ b_0, b_1, b_2, \dots, b_n \end{aligned}$$

суть цѣлыя числа.

Для краткости мы будемъ называть такія функціи просто функціями. Впрочемъ, если намъ придется разсматривать не цѣлыя функціи или цѣлыя функціи но не съ цѣлыми коэффициентами, то мы каждый разъ будемъ дѣлать оговорку.

Функціи называются *сравнимыми по некоторому модулю p* , если коэффициенты при одинаковыхъ степеняхъ x сравнимы по модулю p ; такъ что

$$(1) \quad A \equiv B \pmod{p};$$

если

$$\left. \begin{aligned} a_0 &\equiv b_0 \\ a_1 &\equiv b_1 \\ a_2 &\equiv b_2 \\ \dots \dots \dots \end{aligned} \right\} \pmod{p}$$

Если

$$A \equiv 0 \pmod{p},$$

то всѣ коэффициенты A дѣлятся на p .

Извѣстно², что если въ двухъ сравнимыхъ функціяхъ переменной x дать одно и тоже значеніе или значенія различныя но сравнимыя, то и результаты выйдутъ сравнимыя по тому же модулю.

Надъ сравненіями вида (1) можно дѣлать такія же дѣйствія какъ и надъ обыкновенными сравненіями.

Такъ, если

$$A \equiv B, \quad C \equiv D, \quad E \equiv F \pmod{p},$$

то имѣютъ мѣсто также и сравненія

$$\left. \begin{aligned} A + C + E &\equiv B + D + F \\ A - C &\equiv B - D \\ ACE &\equiv BDF \\ \text{и т. п.,} \end{aligned} \right\} \pmod{p}$$

доказательство которыхъ не представляетъ никакихъ затрудненій.

2.

Далѣе мы будемъ предполагать модуль p числомъ простымъ. Пусть A и B будутъ двѣ данныя функціи. Если можно подыскать другія двѣ функціи C и D такъ, чтобы имѣло мѣсто тождество

$$BC = A + pD$$

или, что тоже самое, сравненіе

$$BC \equiv A \pmod{p},$$

то говорить, что *функція A дѣлится по модулю p на функцію B* , а C есть частное отъ этого дѣленія; другими словами: *функція A равна по модулю p произведенію двухъ функцій B и C* .

Предполагая, что B не дѣлится на p , мы докажемъ, что частное C имѣетъ одно определенное значеніе, при этомъ конечно, всѣ функціи сравнимы съ C по модулю p считаются за одну. Дѣйствительно, допустимъ, что кромѣ функцій C будетъ существовать еще другая C' , удовлетворяющая сравненію

$$BC' \equiv A \pmod{p}$$

и не сравнимая съ C по модулю p . Въ такомъ случаѣ мы получимъ

$$(1) \quad B(C' - C) \equiv 0 \pmod{p}.$$

Такъ какъ, по предположенію, ни одна изъ функцій B и $C' - C$ не дѣлится на p , то отбросивъ въ этихъ функціяхъ члены дѣлящіеся на p и разложивъ остатки по визходящимъ степенямъ x будемъ имѣть

$$\left. \begin{aligned} C' - C &\equiv cx^g + \dots \\ B &\equiv bx^f + \dots \end{aligned} \right\} \pmod{p},$$

гдѣ коэффициенты b и c не дѣлятся на p ; точками обозначены члены степеней соотвѣтственно меньшихъ f и g .

Положивши это, получимъ

$$B(C' - C) \equiv bcx^{f+g} + \dots \pmod{p};$$

слѣдовательно произведеніе $B(C' - C)$ не дѣлится на p , а это противорѣчитъ сравненію (1).

Чтобы на самомъ дѣлѣ раздѣлить A на B можно поступать слѣдующимъ образомъ:

Прежде всего можно отбросить въ этихъ функціяхъ члены, коэффициенты которыхъ дѣлятся на p и замѣнить остальные коэффициенты другими числами сравнимыми съ ними по модулю p , если найдемъ это удобнымъ. Послѣ этихъ преобразованій функціи A и B замѣнятся функціями A' и B' , такъ что

$$A \equiv A', \quad B \equiv B' \pmod{p}.$$

Пусть b будетъ коэффициентъ высшаго члена B' , который, по предположенію, уже не будетъ дѣлиться на p . По числу b мы найдемъ β удовлетворяющее сравненію

$$\beta b \equiv 1 \pmod{p}$$

и составимъ функцію

$$(2) \quad B'' \equiv \beta B' \pmod{p},$$

коэффициентъ высшаго члена которой можно принять равнымъ единицѣ

Затѣмъ мы дѣлимъ A' на B'' алгебраически, отбрасывая въ каждомъ полученномъ остаткѣ члены съ коэффициентами дѣлящимися на p и замѣняя коэффициенты другихъ членовъ ихъ вычетами по модулю p , если найдемъ это удобнымъ. Поступая такимъ образомъ мы непремѣнно придемъ къ остатку степени ниже степени B' . Для того чтобы A' или, что все равно, A дѣлилось по модулю p на B'' необходимо и достаточно, чтобы этотъ остатокъ дѣлился на p . Обозначивъ черезъ C' частное отъ дѣленія A' на B'' , получимъ

$$A \equiv A' \equiv B'' C' \equiv b B' \cdot \beta C' \pmod{p}.$$

Но изъ (2) выводимъ

$$b B' \equiv B' \equiv B \pmod{p}.$$

Положивъ поэтому

$$\beta C' \equiv C \pmod{p},$$

будемъ имѣть

$$A \equiv B C \pmod{p}.$$

Примѣчаніе. Если функціи A и B дѣлятся на функцію C по модулю p , то, очевидно, и $A \pm B$ дѣлится на C . Точно также, если функція A дѣлится на функцію C по модулю p и B есть какая нибудь другая функція, то и произведеніе AB дѣлится на C по модулю p .

3.

Рѣшимъ теперь такую задачу:

Даны двѣ функціи A и B , найти ихъ общій наибольшій дѣлитель по модулю p т. е. дѣлитель наивысшей степени Пусть A будетъ степени не ниже чѣмъ B ; дѣлимъ A на B по модулю p . Если дѣленіе совершится безъ остатка, то B и будетъ общимъ наибольшимъ дѣлителемъ. Въ противномъ случаѣ мы получимъ остатокъ C степени ниже чѣмъ B . Дѣлимъ теперь B на C и т. д.

Такъ что получимъ рядъ сравненій

$$A \equiv aB + C, \quad B \equiv bC + D, \quad C \equiv cD + E \text{ и т. д. } \pmod{p}.$$

Функции $A, B, C, D, E \dots$ будут степеней все убывающих.

Если мы дойдем до такой функции, что деление на нее совершится без остатка, то эта функция и будет общим наибольшим делителем A и B . Например, если D будет делиться на E , то E и будет общим наибольшим делителем. Действительно, из предыдущих равенств видно, что тогда C, B и A будут делиться на E по модулю p ; следовательно E будет общим делителем A и B . Во вторых из тех же равенств видно, что общий наибольший делитель A и B должен делиться по модулю p все функции

$$C, D, E$$

и следовательно он не может быть степени выше чем E . Отсюда видно, что функция E или вообще функция λE , где λ есть число не делящееся на p и будет общим наибольшим делителем по модулю p функций A и B .

Если мы не дойдем до такой функции, что деление совершится без остатка, то мы непременно придем к остатку неравному нулю по модулю p и не содержащему x . В таком случае функции A и B не будут иметь общего делителя и мы назовем их *взаимно-простыми по модулю p* .

Примечание. Если A и B имеют общего наибольшего делителя λE , то число λ лучше всего выбрать так, чтобы коэффициент высшего члена λE был сравним с единицею по модулю p , что всегда возможно, потому что в функции λE можно выбросить все члены, коэффициенты которых делятся на p .

4.

Теорема. Если A и B суть функции взаимно простые по модулю p , то всегда можно найти такие функции P и Q , что

$$PA - QB \equiv 1 \pmod{p}.$$

Доказат. Произведем над функциями A и B то действие, при помощи которого ищется общий наибольший делитель. Пусть

$$A \equiv aB + C, \quad B \equiv bC + D \text{ и т. д. } K \equiv kL + M \pmod{p},$$

где M есть число независимое от x .

Составляем теперь ряд функций

$$\begin{aligned} a, a', a'', \dots a^{(\lambda)} \\ 1, b, b', \dots b^{(\lambda-1)}, \end{aligned}$$

которые суть числители и знаменатели последовательных подходящих дробей непрерывной дроби

$$a + \frac{1}{b + \frac{1}{c + \dots \frac{1}{g + \frac{1}{k}}}}$$

Такъ что

$$\begin{aligned} a' &= ab + 1, & a'' &= ca' + a, & a''' &= da'' + a' \text{ и т. д.} \\ b' &= bc + 1, & b'' &= db' + b \end{aligned}$$

При этомъ будемъ имѣть

$$A - aB = C, -bA - a'B = bC - B = -D \text{ и т. д.}$$

и наконецъ

$$b^{(\lambda-1)} A - a^{(\lambda)} B = \pm M.$$

Пусть теперь μ будетъ такое число, что

$$\pm \mu M \equiv 1 \pmod{p}.$$

Положивъ

$$\mu b^{(\lambda-1)} \equiv P, \quad \mu a^{(\lambda)} \equiv Q \pmod{p},$$

получимъ

$$PA - QB \equiv 1 \pmod{p}.$$

Изъ доказанной теоремы выводятся такія же слѣдствія какъ и изъ подобной теоремы для цѣлыхъ чиселъ.

Слѣдствіе. Если M есть общій наибольшій дѣлитель A и B , то всегда можно найти такія двѣ цѣлыя функціи P и Q , что

$$PA - QB \equiv M \pmod{p}.$$

5.

Теорема. Если функція A , простая относительно B по модулю p , дѣлитъ произведеніе BC по этому модулю, то она дѣлитъ также и функцію C .

Доказат. Пусть P и Q будутъ функціи удовлетворяющія сравненію (n°4)

$$(1) \quad PA - QB \equiv 1 \pmod{p}$$

и пусть

$$BC \equiv AD \pmod{p}.$$

Умноживъ обѣ части сравненія (1) на C , получимъ

$$(PC - QD) A \equiv C \pmod{p}.$$

Изъ этого сравненія видно, что C дѣлится на A по модулю p .

Слѣдствіе. Если функція A взаимно простая съ B и C по модулю p , то она также будетъ простая и относительно произведенія BC .

6.

Функція недѣлящаяся по модулю p ни на какую функцію степени низшей называется *простою по этому модулю*³. Напримѣръ

$$x^2 + 1, \quad x^3 + 2$$

суть простыя функціи по модулю 7.

Если A будетъ какая нибудь простая функція по модулю p , то и λA , гдѣ λ означаетъ какое нибудь цѣлое число не дѣлящееся на p , будетъ также простая функція. Всѣ эти функціи мы будемъ считать за одну. Число λ можно выбрать такъ, чтобы коэффициентъ высшаго члена функціи λA былъ сравнимъ съ единицею по модулю p .

Изъ доказанной выше теоремы ($n^\circ 5$) слѣдуютъ такіа:

Теорема. Если простая функція A по модулю p дѣлится по этому модулю произведеніемъ функцій $B, C, D, \dots$, то она дѣлится однимъ изъ множителей $B, C, D, \dots$.

Теорема. Если простая по модулю p функція A не дѣлится по этому модулю ни одной изъ функцій $B, C, D, \dots$, то она не можетъ дѣлиться и ихъ произведеніемъ $B, C, D, \dots$.

7.

Если функція A не есть простая по модулю p , то ее можно разложить на произведеніе простыхъ. Дѣйствительно, такъ какъ A не есть простая функція по модулю p , то она должна дѣлиться по этому модулю на нѣкоторую функцію B степени низшей и т. д. Понятно, что разсуждая такимъ образомъ мы непремѣнно дойдемъ до нѣкоторой простой функціи L , которая будетъ дѣлится A ; такъ что

$$A \equiv LA_1 \pmod{p},$$

гдѣ A_1 степени ниже чѣмъ A . Если A_1 не есть простая функція, то опять можно положить

$$A_1 \equiv L_1 A_2 \pmod{p},$$

гдѣ L_1 есть простая функція и A_2 степени ниже чѣмъ A_1 и т. д. Очевидно изъ этого, что A можно представить въ видѣ

$$A \equiv LL_1 L_2 \dots \pmod{p},$$

гдѣ $L, L_1, L_2, \dots$ суть простые функціи.

Докажемъ теперь, что существуетъ только одно разложеніе на простые множители. Дѣйствительно, пусть кромѣ разложенія

$$A \equiv LL_1 L_2 \dots \pmod{p}$$

существуетъ еще другое

$$A \equiv MM_1 M_2 \dots \pmod{p};$$

слѣдовательно

$$LL_1 L_2 \dots \equiv MM_1 M_2 \dots \pmod{p}$$

т. е.

$$(1) \quad LL_1 L_2 \dots \equiv MM_1 M_2 \dots + pN,$$

гдѣ N есть нѣкоторая функція x .

Такъ какъ изъ этого равенства слѣдуетъ, что простая функція L должна дѣлиться по модулю p произведеніемъ $MM_1 M_2 \dots$, то между простыми функціями $M, M_1, M_2, \dots$ есть хотя