Е. Золотарев

Теория целых комплексных чисел с приложением к интегральному исчислению

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Е11

Е. Золотарев
Е11 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

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 логариѳмахъ и поэтому относится къ той части интегральнаго исчисленія, которая обогащена изслѣдованіями Абеля, Ліувилля, 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.

ОГЛАВЛЕНІЕ.

Глава I.

О функціональныхъ сравненіяхъ.

Глава II.

О комплексныхъ единицахъ.

Глава III.

Идеальные множители комплексныхъ чиселъ.

Глава IV.

Приложеніе теоріи комплексныхъ чиселъ къ одному вопросу интегральнаго ис·

VI.

ГЛАВА I.

О функціональныхъ сравненіяхъ[1].

1.

Пусть A и B будутъ двѣ функціи перемѣнной x вида

$$a_0 + a_1x + a_2x^2 + \ldots + a_mx^m$$
$$b_0 + b_1x + b_2x^2 + \ldots + b_nx^n,$$

гдѣ коэффиціенты

$$a_0,\ a_1,\ a_2,\ \ldots\ a_m$$
$$b_0,\ b_1,\ b_2,\ \ldots\ b_n$$

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 коэффиціентами, то мы каждый разъ будемъ дѣлать оговорку.

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

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

если

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

Если

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

то всѣ коэффиціенты A дѣлятся на p.

Извѣстно[2], что если въ двухъ сравнимыхъ функціяхъ перемѣнной x дать одно и тоже значеніе или значенія различныя но сравнимыя, то и результаты выйдутъ сравнимые по тому же модулю.

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

Такъ, если

$$A \equiv B,\ C \equiv D,\ E \equiv F \ (\text{мод. } p),$$

то имѣютъ мѣсто также и сравненія

$$\left.\begin{array}{c} A + C + E \equiv B + D + F \\ A - C \equiv B - D \\ ACE \equiv BDF \\ \text{. и т п.,} \end{array}\right\} (\text{мод. } p)$$

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

$$BC \equiv A \ (\text{мод. } p),$$

то говорятъ, 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 опредѣленное значеніе, при этомъ конечно, всѣ функціи сравнимыя съ C по модулю p считаются за одну. Дѣйствительно, допустимъ, что кромѣ функціи C будетъ существовать еще другая C', удовлетворяющая сравненію

$$BC' \equiv A \ (\text{мод. } p)$$

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

$$B(C' - C) \equiv 0 \ (\text{мод. } p). \tag{1}$$

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 низходящимъ степенямъ x будемъ имѣть

$$\left.\begin{array}{c} C' - C \equiv cx^g + \ldots . \\ B \equiv bx^f + \ldots . \end{array}\right\} (\text{мод. } p),$$

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

Положивши это, получимъ

$$B(C' - C) \equiv bcx^{f+g} + \ldots . \ (\text{мод. } p);$$

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, коеффиціенты которыхъ дѣлятся на p и замѣнить остальные коеффиціенты 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 коеффиціентъ высшаго члена B', который, по предположенію, уже не будетъ дѣлится на p. По числу b мы найдемъ β удовлетворяющее сравненію

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

и составимъ функцію

$$B'' \equiv \beta B' \pmod{p}, \tag{2}$$

коеффиціентъ высшаго члена которой можно принять равнымъ единицѣ

Затѣмъ мы дѣлимъ A' на B'' алгебраически, отбрасывая въ каждомъ полученномъ остаткѣ члены съ коеффиціентами дѣлящимися на p и замѣняя коеффиціенты 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

$$A \equiv A' \equiv B''C' \equiv bB'' \,.\, \beta C' \pmod{p}.$$

Но изъ (2) выводимъ

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

Положивъ поэтому

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

будемъ имѣть

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

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

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

Функціи A, B, C, D, E . . . . будутъ степеней все убывающихъ.

Если мы дойдемъ до такой функціи, что дѣленіе на нее совершится безъ остатка, то эта функція и будетъ общимъ наибольшимъ дѣлителемъ A и B. Напримѣръ, если D будетъ дѣлиться на E, то E и будетъ общимъ наибольшимъ дѣлителемъ. Дѣйствительно, изъ предыдущихъ равенствъ видно, что тогда C, B и A будутъ дѣлиться на E по модулю p; слѣдовательно E будетъ общимъ дѣлителемъ A и B. Во вторыхъ изъ тѣхъ же равенствъ видно, что общій наибольшій дѣлитель A и B долженъ дѣлить по модулю p всѣ функціи

$$C,\ D,\ E$$

и слѣдовательно онъ не можетъ быть степени выше чѣмъ E. Отсюда видно, что функція E или вообще функція λE, гдѣ λ есть число не дѣлящееся на p и будетъ общимъ наибольшимъ дѣлителемъ по модулю p функцій A и B.

Если мы не дойдемъ до такой функціи, что дѣленіе совершится безъ остатка, то мы непремѣнно придемъ къ остатку неравному нулю по модулю p и не содержащему x. Въ такомъ случаѣ функціи A и B не будутъ имѣть общаго дѣлителя и мы назовемъ ихъ *взаимно-простыми по модулю* p.

Примѣчаніе. Если A и B имѣютъ общаго наибольшаго дѣлителя λE, то число λ лучше всего выбрать такъ, чтобы коеффиціентъ высшаго члена λE былъ сравнимъ съ единицею по модулю p, что всегда возможно, потому что въ функціи λE можно выбросить всѣ члены, коеффиціенты которыхъ дѣлятся на p.

4.

Теорема. *Если A и B суть функціи взаимно простыя по модулю p, то всегда можно найти такія функціи P и Q, что*

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

Доказат. Произведемъ надъ функціями A и B то дѣйствіе, при помощи котораго ищется общій наибольшій дѣлитель. Пусть

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

гдѣ M есть число независящее отъ x.

Составляемъ теперь рядъ функцій

$$a,\ a',\ a'',\ \ldots\ a^{(\lambda)}$$
$$1,\ b,\ b',\ \ldots\ b^{(\lambda-1)},$$

которыя суть числители и знаменатели послѣдовательныхъ подходящихъ дробей непрерывной дроби

$$a + \cfrac{1}{b + \cfrac{1}{c + \ddots \cfrac{1}{g + \cfrac{1}{k}}}}$$

Такъ что

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

При этомъ будемъ имѣть

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

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 ($n^0 4$)

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

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 недѣлящееся на p, будетъ также простая функція. Всѣ эти функціи мы будемъ считать за одну. Число λ можно выбрать такъ, чтобы коеффиціентъ высшаго члена функціи λA былъ сравнимъ съ единицею по модулю p.

Изъ доказанной выше теоремы (n^0 5) слѣдуютъ такія:

Теорема. *Если простая функція A по модулю p дѣлитъ по этому модулю произведеніе функцій BCD . . . , то она дѣлитъ одинъ изъ множителей B, C, D, ...*

Теорема. *Если простая по модулю p функція A не дѣлитъ по этому модулю ни одной изъ функцій B, C, D. . . . , то она не можетъ дѣлить и ихъ произведенія BCD. . . .*

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 дѣлить 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

$$A \equiv LL_1L_2 \ldots . \pmod{p},$$

гдѣ L, L_1, L_2 . . . . суть простыя функціи.

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

$$A \equiv LL_1L_2 \ldots . \pmod{p}$$

существуетъ еще другое

$$A \equiv MM_1M_2 \ldots . \pmod{p};$$

слѣдовательно

$$LL_1L_2 \ldots . \equiv MM_1M_2 \ldots . \pmod{p}$$

т. е.

$$LL_1L_2 \ldots . \equiv MM_1M_2 \ldots . + pN, \tag{1}$$

гдѣ N есть нѣкоторая функція x.

Такъ какъ изъ этого равенства слѣдуетъ, что простая функція L должна дѣлить по модулю p произведеніе $MM_1M_2 \ldots .$, то между простыми функціями M, M_1, M_2 . . . . есть хотя