

ТЕОРИЯ
ЦѢЛЫХЪ
КОМПЛЕКСНЫХЪ ЧИСЕЛЬ
СЪ ПРИЛОЖЕНИЕМЪ

ЕВ

ИНТЕГРАЛЬНОМУ ИСЧИСЛЕНИЮ

СОЧИНЕНИЕ

Е. Золотарева.



С.-ПЕТЕРБУРГЪ.

Типографія А. Яковсона (Вас. Остр., 9 лин. домъ № 8).

1874.

По определению физико-математического факультета С.-Петербургского Университета
печатать дозволяется. С.-Петербургъ, 23 Ноября 1873 года.

Деканъ *A. Бекетовъ*.

ПРЕДИСЛОВІЕ.

Въ этомъ сочиненіи разматриваются комплексныя числа, зависящія отъ корней какого нибудь неприводимаго уравненія съ цѣлыми коефиціентами, изъ которыхъ первый равенъ единицѣ. Цѣлыми комплексными числами здѣсь называются цѣлые функціи съ цѣлыми коефиціентами, зависящія отъ одного изъ корней такого уравненія. Относительно такихъ чиселъ сами собой представляются различные вопросы о дѣлимости, о разложеніи на множители и т. д. Рѣшенія этихъ вопросовъ интересны въ особенности по тѣмъ разнообразнымъ приложеніямъ, которыя они встрѣчаютъ въ теоріи чиселъ, высшей алгебрѣ и интегральномъ исчислѣніи. Можно сказать, что теорія комплексныхъ чиселъ есть одна изъ тѣхъ, которыя соединяютъ названныя, по видимому столь различные, части математического анализа, что, конечно, составляеть одну изъ привлекательныхъ сторонъ этого предмета. Вотъ почему, какъ намъ кажется, мы встрѣчаемся здѣсь съ именами такихъ великихъ геометровъ, какъ Гауссъ, Дирихле, Куммеръ, Эрмитъ, Кронеккеръ и Ейзенштейнъ.

Исходною точкою при составленіи теоріи комплексныхъ чиселъ мнѣ послужили свойства функциональныхъ сравненій, или, точнѣе, свойства полиномовъ съ цѣлыми коефиціентами относительно нѣкотораго простаго модуля. Уже въ 1797 или 1798 году Гауссу были известны главнѣйшія свойства этихъ сравненій. По извлечению изъ оставленной имъ рукописи, которое находится во II-мъ томѣ его сочиненій, видно, что изложеніе свойствъ функциональныхъ сравненій должно было составить VIII главу его «*Disquisitiones arithmeticæ*». Впослѣдствіи эти свойства были вновь найдены СЕРРЕ, который подробно развилъ ихъ въ своемъ курсѣ высшей алгебры и приложилъ къ теоріи уравненій.

Но самое естественное и замѣчательное приложеніе свойствъ функциональныхъ сравненій встречается въ теоріи комплексныхъ чиселъ. Это и вполнѣ понятно, такъ какъ относительно комплексныхъ чиселъ приходится рѣшать задачи, имѣющія много общаго съ тѣми, которые рѣшаются въ теоріи функциональныхъ сравненій.

Для того, чтобы нагляди^{ть} выставить эту связь, а также для того, чтобы показать теоремы въ томъ самомъ видѣ, въ какомъ онъ мнѣ нужны для приложенийъ, я счелъ полезнымъ посвятить первую главу своего сочиненія изложению свойствъ функциональныхъ сравненій.

Комплексныя числа имѣютъ ту особенность сравнительно съ обыкновенными цѣлыми числами, что существуетъ вообще безчисленное множество комплексныхъ чиселъ дѣлящихъ единицу. Эти числа называются комплексными единицами и играютъ существенную роль въ теоріи комплексныхъ чиселъ. Свойства ихъ главнымъ образомъ были изучены Дирихле.

Во II-й главѣ своего сочиненія я излагаю какъ результаты, найденные Дирихле, такъ и иѣкоторые другие, принадлежащіе Куммеру и Кронеккеру. Я основываю свои доказательства на теоремѣ Эрмита относительно предѣла \min_{α} опредѣленной квадратичной формы въ функции опредѣлителя. Эта прекрасная теорема, замѣняющая въ общемъ случаѣ непрерывныя дроби, имѣеть въ высшей степени важное значеніе въ теоріи чиселъ.

III-я глава посвящена изложению свойствъ идеальныхъ множителей комплексныхъ чиселъ. Въ ней я обобщаю извѣстную теорію Куммера для комплексныхъ чиселъ, зависящихъ отъ корней изъ единицы. Желая представить теорію идеальныхъ множителей въ самомъ простомъ видѣ, я отложилъ до другаго раза публикацию моихъ изслѣдований относительно тѣхъ уравненій, для которыхъ приведенное выше понятіе о цѣломъ комплексномъ числѣ является недостаточнымъ. Такъ что, если рассматривать только уравненія, для которыхъ можно ограничиться предыдущимъ опредѣленіемъ цѣлыхъ комплексныхъ чиселъ, то изложенную здѣсь теорію нужно считать законченной.

При этомъ я считаю необходимымъ упомянуть о двухъ работахъ, которые имѣютъ иѣкоторыя пункты соприосновенія съ мою. Первая изъ нихъ принадлежитъ Зеллингу (*Zeitschrift für Mathematik und Physik herausgegeben von O. Schlömilch 1865*). Это первая попытка обобщить идеальные числа Куммера, но такъ какъ она основана на иѣкоторыхъ опредѣленіяхъ, при помощи которыхъ трудности обходятся, но не устраняются и на иѣкоторыхъ допущеніяхъ, которые не оправданы никакими приложеніями, то ее нельзя считать удовлетворительною. Другая работа, во многихъ отношеніяхъ весьма замѣчательная, принадлежитъ Дедекинду. (*Vorlesungen über Zahlentheorie. Lejeune Dirichlet. 2-е изданіе, статья «Composition der Formen»*). Она не представляетъ собственно теоріи цѣлыхъ комплексныхъ чиселъ. Цѣль Дедекинда разсмотреть идеальные множители съ болѣе высокой точки зренія. Однакоже, что касается собственно комплексныхъ чиселъ, мы должны сказать относительно этой работы тоже, что и о работѣ Зеллинга.

Въ IV-й главѣ я прилагаю теорію комплексныхъ чиселъ къ одному вопросу интегрального исчислениѧ. 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 интегрального исчислениѧ, 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 исчислениемъ и теоріею чиселъ.

Е. З.

ОГЛАВЛЕНИЕ.

Глава I.

nn⁰ О функциональныхъ сравненіяхъ.

1. Определение функциональныхъ сравнений.
2. Дѣлимость одной функциї на другую по нѣкоторому простому модулю.
3. Объ общемъ наибольшемъ дѣлителѣ двухъ функций по нѣкоторому простому модулю.
4. Одна теорема относительно двухъ функций взаимно простыхъ до нѣкоторому простому модулю.
5. О дѣлимости произведения двухъ функций по нѣкоторому простому модулю.
6. О простыхъ функцияхъ по нѣкоторому простому модулю.
7. О разложении функций на простые множители по нѣкоторому простому модулю.
8. Отдѣленіе кратныхъ множителей.
9. О сравненіяхъ по нѣкоторому простому модулю и нѣкоторой простой функции.
- 10. Теорема относящаяся къ такимъ сравненіямъ.
11. Теорема аналогичная теоремѣ Фермата.
12. Другая теорема, дополняющая предыдущую.
13. О числѣ простыхъ функций данной степени по нѣкоторому простому модулю.
14. Дополненіе относительно разложения функций на простые множители по нѣкоторому простому модулю.
15. О функциї $\frac{x^n - 1}{x - 1}$.
- 16 — 19. О периодахъ.
20. Разложение функциї $\frac{x^n - 1}{x - 1}$ на простые множители по нѣкоторому простому модулю, при n простомъ.
21. Примѣръ.

Глава II.

О комплексныхъ единицахъ.

22. Общія замѣчанія о комплексныхъ числахъ.
23. Сопряженные комплексные числа. Норма комплексныхъ чиселъ. Союзное комплексное число.
24. О дѣйствіяхъ надъ комплексными числами.
25. Определение комплексныхъ единицъ.
26. Лемма относительно линейныхъ функций, зависящихъ отъ цѣлыхъ чиселъ.
27. Другая лемма относительно линейныхъ функций.
28. Объ уравненіи $N_{\varphi}x = 1$; особенные рѣшенія этого уравненія.
29. Объ уравненіи $N_{\varphi}x = T$.
30. Приложеніе теоремы, доказанной въ предыдущемъ n⁰, къ рѣшенію уравненія $N_{\varphi}x = 1$.

nn^o

31. Определение независимых решений.
 32. Доказательство существования системы, состоящей из $h - 1$ независимых решений уравнения $N_r x = 1$.
 33 — 34. Различные теоремы, относящиеся к этой системе решений.
 35. Объект основных решений уравнения $N_r x = T$.
 36. Общее выражение всех основных решений.
 37. Решения уравнения $N_r x = r$.
 38. Общая формула для комплексных единиц.

Глава III.

Идеальные множители комплексных чисел.

39. Краткая историческая замечания о комплексных числах.
 40. О делимости произведений нескольких комплексных чисел на обыкновенное простое число.
 41 — 42. О делимости нормы комплексного числа на обыкновенное простое число.
 43. Замечания об объекте основного уравнения $F(x) = 0$.
 44. Постановка главного вопроса, решение которого содержится в этой главе.
 45. Классификация комплексных чисел на простые и сложные.
 46. Определение степени кратности простого идеального множителя существующего комплексного числа.
 47 — 49. Теоремы относительно идеальных чисел.
 50. Свойство нормы комплексных чисел.
 51 — 53. Разложение комплексных чисел на простые идеальные множители.
 54 — 55. Частные случаи комплексных чисел.
 56 — 60. Распределение идеальных комплексных чисел на классы.

Глава IV.

Приложение теории комплексных чисел к одному вопросу интегрального ис-

61. Постановка вопроса и некоторые исторические замечания об интегрировании алгебраических дифференциалов в логарифмах.

62 — 64. Приведение дифференциала $\frac{(x + A) dx}{\sqrt{x^4 + \gamma x^3 + \delta x^2 + \varepsilon x + \zeta}}$ к виду $\frac{(x + A) dx}{\sqrt{x(x - 1)(x - \alpha)(x - \beta)}}$.

65. Выражение $\int_0^x \frac{(x + A) dx}{\sqrt{x(x - 1)(x - \alpha)(x - \beta)}}$ в эллиптических функциях.

66. Применение преобразования n^o 63 к дифференциальному $\frac{(x + A) dx}{\sqrt{x(x - 1)(x - \alpha)(x - \beta)}}$.

67. Тоже преобразование в эллиптических функциях.

68. Применение к дифференциальному $\frac{(x + A) dx}{\sqrt{x(x - 1)(x - \alpha)(x - \beta)}}$ преобразования n^o 64.

69. Тоже преобразование в эллиптических функциях.

70. Условие интегрируемости дифференциала $\frac{(x + A) dx}{\sqrt{x(x - 1)(x - \alpha)(x - \beta)}}$ в логарифмах.

71. Объект уравнения $F(x, \beta) = 0$ между параметрами α и β .

72. Другой вид условий интегрируемости

VI.

нн°

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

74. Три различные случаи при решеніи 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 рациональными функціями одного параметра.

76 — 82 Решеніе задачи въ третьемъ случаѣ.

83. Примѣры.

84 — 88. Прибавленіе.

ГЛАВА I.

О функціональныхъ сравненіяхъ¹.

1.

Пусть A и B будутъ двѣ функціи переменной x вида

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

гдѣ коефиціенты

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

суть цѣлые числа.

Для краткости мы будемъ называть такія функціи просто функціями. Впрочемъ, если наль придется разматривать не цѣлые функціи или цѣлые функціи но не съ цѣлыми коефиціентами, то мы каждый разъ будемъ дѣлать оговорку.

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

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

если

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

Если

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

то всѣ коефиціенты 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 сравнимые 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

$$\left. \begin{array}{l} A + C + E \equiv B + D + F \\ A - C \equiv B - D \\ ACE \equiv BDF \end{array} \right\} \pmod{p}$$

и т. д.,

доказательство которыхъ не представляетъ никакихъ затрудненій.

2.

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

$$BC = A + pD$$

или, что тоже самое, сравненіе

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

то говорятъ, что *функция A дѣлится по модулю p на функцию B*, а C есть частное отъ этого дѣленія; другими словами: *функция A равна по модулю p произведению двухъ функций B и C*.

Предполагая, что B не дѣлится на p , мы докажемъ, что частное C имѣть одно определенное значение, при этомъ конечно, всѣ функции сравнимы съ C по модулю p считаются за одну. Дѣйствительно, допустимъ, что кроме функции 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 функций B и $C' - C$ не дѣлится на p , то отбросивъ въ этихъ функцияхъ члены дѣлящіеся на p и разложивъ остатки по низходящимъ степенямъ x будемъ имѣть

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

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

Положивши это, получимъ

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

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

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

Прежде всего можно отбросить въ этихъ функцияхъ члены, коефиціенты которыхъ дѣлятся на p и замѣнить остальные коефиціенты другими числами сравнимыми съ ними по модулю p , если найдемъ это удобнымъ. Послѣ этихъ преобразованій функции A и B замѣняются функциями A' и B' , такъ что

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

Пусть b будетъ коефиціентъ 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 функцию

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

коефиціентъ высшаго члена которой можно принять равнымъ единицѣ

Затѣмъ мы дѣлимъ A' на B'' алгебраически, отбрасывая въ каждомъ полученному остатку члены съ коефиціентами дѣлящимися на p и замѣняя коефиціенты другихъ членовъ ихъ вычетами по модулю p , если найдемъ это удобнымъ. Поступая такимъ образомъ мы неизрѣдно приDEMЪ 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

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

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 функции A и B дѣлятся на функцию C по модулю p , то, очевидно, и $A \pm B$ дѣлится на C . Точно также, если функция A дѣлится на функцию C по модулю p и B есть какая нибудь другая функция, то и произведеніе AB дѣлится на C по модулю p .

3.

Рѣшимъ теперь такую задачу:

Даны двѣ функции A и B , найти ихъ общий 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 совершился 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

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

Функції $A, B, C, D, E \dots$ будуть степеней все убывающихъ.

Если мы дойдемъ до такой функциї, что дѣленіе на нее совершится безъ остатка, то эта функция 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 ; следовательно E будетъ общимъ дѣлителемъ A и B . Во вторыхъ изъ тѣхъ же равенствъ видно, что общий наибольший дѣлитель A и B долженъ дѣлить по модулю p всѣ функции

$$C, D, E$$

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

Если мы не дойдемъ до такой функциї, что дѣленіе совершится безъ остатка, то мы непремѣнно приDEMЪ къ остатку неравному нулю по модулю p и не содержащему x . Въ такомъ случаѣ функции 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 выбратьъ такъ, чтобы коефиціентъ высшаго члена λE былъ сравнимъ съ единицею по модулю p , что всегда возможно, потому что въ функции λE можно выбросить всѣ члены, коефиціенты которыхъ дѣлятся на p .

4.

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

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

Доказат. Произведемъ надъ функциями A и B то дѣйствіе, при помощи котораго ищется общий наибольший 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 функций

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

которые суть числители и знаменатели послѣдовательныхъ подходящихъ дробей непрерывной дроби

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

Такъ что

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

При этомъ будемъ имѣть

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

и наконецъ

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

Пусть теперь μ будеть 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 цѣлые функциіи P и Q , что

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

5.

Теорема. Если функция A , простая относительно B по модулю p , дѣлить произведение BC по этому модулю, то она дѣлить также и функцию C .

Доказат. Пусть P и Q будутъ функциіи 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 функция A взаимно простая съ B и C по модулю p , то она также будетъ простая и относительно произведения BC .

6.

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

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

суть простыя функциіи по модулю 7.

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

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

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

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

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 непрерѣнно 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

$$A \equiv LL_1L_2 \dots \pmod{p},$$

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

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

$$A \equiv LL_1L_2 \dots \pmod{p}$$

существуетъ еще другое

$$A \equiv MM_1M_2 \dots \pmod{p};$$

слѣдовательно

$$LL_1L_2 \dots \equiv MM_1M_2 \dots \pmod{p}$$

т. е.

$$(1) \quad LL_1L_2 \dots \equiv MM_1M_2 \dots + pN,$$

гдѣ N есть нѣкоторая функція x .

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

одна сравнимая съ L по модулю p . Пусть $M = L + pQ$. Внося эту величину въ равенство (1), найдемъ

$$LL_1L_2\ldots = LM_1M_2\ldots + pN_1.$$

Отсюда ясно, что функция N_1 должна дѣлиться на L . Положивъ $N_1 = LN_2$, получимъ

$$L_1L_2\ldots = M_1M_2\ldots + pN_2.$$

Продолжая тоже разсужденіе далѣе, увидимъ, что множители $M_1, M_2\ldots$ отличаются только порядкомъ отъ L_1, L_2, \dots .

Можетъ случиться, что при разложеніи A на простыя функции какія нибудь функции $L, L_1\ldots$ войдутъ нѣсколько разъ множителями. Такъ что вообще можно положить

$$A \equiv L^n L_1^{n_1} L_2^{n_2} \ldots \pmod{p},$$

гдѣ $n, n_1, n_2\ldots$ цѣлыя положительныя числа.

8.

Въ томъ случаѣ, когда функция имѣеть кратныхъ множителей по модулю p , она и ея первая производная, какъ мы увидимъ, имѣютъ общаго дѣлителя по этому модулю. На основаніи этого свойства можно отдѣлить нѣкоторые множители A при помощи алгебраического дѣленія, подобно тому какъ отдѣляются кратные корни въ алгебраическихъ уравненіяхъ.

Мы докажемъ слѣдующую теорему:

Теорема. *Если функция $A \equiv L^n L_1^{n_1} \ldots L_\lambda^{n_\lambda} \pmod{p}$, ідѣ $L, L_1\ldots L_\lambda$ простыя функции и $n, n_1, \ldots n_\lambda$ цѣлыя числа, то A будетъ имѣть общихъ дѣлителей по модулю p со своею первою производною. Какой нибудь множитель A напр. L войдетъ въ общаго наибольшаго дѣлителя съ показателемъ $n-1$, если n не дѣлится на p и съ показателемъ n , если $n \equiv 0 \pmod{p}$.*

Доказат. Взявъ дѣйствительно первую производную A , получимъ

$$A' \equiv L^{n-1} L_1^{n_1-1} \ldots L_\lambda^{n_\lambda-1} (nL'L_1 \ldots L_\lambda + n_1 LL'_1 \ldots L_\lambda + \ldots + n_\lambda LL_1 \ldots L'_{\lambda-1}) \pmod{p}.$$

Если n не дѣлится на p , то функция стоящая въ скобкахъ не будетъ дѣлиться на L по модулю p , потому что всѣ ея члены дѣлятся на L за исключеніемъ

$$nL'L_1 \ldots L_\lambda,$$

который не можетъ дѣлиться на L , потому что $L_1, L_2\ldots L_\lambda$ суть простыя функции отличныя отъ L , а L' будучи степени ниже чѣмъ L не можетъ дѣлиться на L . Такъ что въ этомъ случаѣ L войдетъ въ общаго наибольшаго дѣлителя съ показателемъ $n-1$. Если же n дѣлится на p , то функция стоящая въ скобкахъ дѣлится на L по модулю p , и въ общаго наибольшаго дѣлителя A и A' войдетъ L^n . Тоже самое можно сказать и относительно другихъ множителей

$$L_1, L_2 \ldots L_\lambda.$$