

**Ю. Сохоцкий**

# **Высшая алгебра**

**Часть 2. Начала теории чисел.**

**Москва  
«Книга по Требованию»**

УДК 93  
ББК 63.3  
Ю11

Ю11 **Ю. Сохоцкий**  
Вышая алгебра: Часть 2. Начала теории чисел. / Ю. Сохоцкий – М.: Книга  
по Требованию, 2021. – 349 с.

**ISBN 978-5-518-00302-6**

**ISBN 978-5-518-00302-6**

© 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.



Серия Книжный Ренессанс

[www.samizday.ru/reprint](http://www.samizday.ru/reprint)



Существуетъ немного примѣровъ своеобразнаго и чрезвычайнаго удачнаго примѣненія трансцендентнаго анализа къ рѣшенію нѣкоторыхъ изъ означенныхъ вопросовъ; подобныя работы, хотя и относятся къ теоріи чиселъ, но составляютъ совершенно отдѣльную ея вѣтвь, выходящую изъ области конечнаго анализа.

Современная теорія чиселъ построена на трехъ началахъ: 1° общій наибольшій дѣлитель (Евклидъ), 2° непрерывныя дроби (Гюгенсъ), 3° начало Дирихле. Настоящая книга посвящена исключительно началу Евклида въ приложеніи къ цѣлымъ числамъ и цѣлымъ функціямъ; потому можно было бы ее озаглавить: „теорія дѣлимости“ или „теорія сравненій“.

Особенное вниманіе было обращено мною на тѣ мѣста, которыя находятъ приложеніе въ дальнѣйшихъ частяхъ алгебры. Такъ, напримѣръ, линейныя сравненія со многими неизвѣстными играютъ существенную роль въ теоріи подстановокъ; потому я останавливаюсь на нихъ немного дольше, чѣмъ Гауссъ въ его „*Disquisitiones arithmeticae*“.

Въ концѣ первой главы я показываю способы рѣшенія въ цѣлыхъ числахъ нѣсколькихъ неопредѣленныхъ уравненій первой степени, которыя могутъ показаться не особенно важными; между тѣмъ въ нихъ содержится рѣшеніе вопроса объ умноженіи такъ называемыхъ идеальныхъ чиселъ (второго порядка) или, все

равно, о сложении квадратичныхъ формъ (Gauss, *compositio formarum*), — одинъ изъ самыхъ плодотворныхъ вопросовъ въ теоріи чиселъ.

Въ общемъ, книга эта представляетъ развитіе моихъ университетскихъ лекцій, на сколько таковое необходимо для основательнаго уразумѣнія высшихъ вопросовъ современной алгебры.

---

# ОГЛАВЛЕНІЕ.

## ГЛАВА I.

Начало общаго наибольшаго дѣлителя. — Первыя приложенія.

### § I. Начало общаго наибольшаго дѣлителя.

	СТР.
1. Нахожденіе общаго наибольшаго дѣлителя двухъ чиселъ и основное его свойство.....	1
2. Случай нѣсколькихъ чиселъ.....	4
3. Понятіе о числахъ взаимно простыхъ.....	4
4. Свойства чиселъ взаимно простыхъ.....	5
5. Понятіе о наименьшемъ кратномъ.....	7

### § II. Разложеніе чиселъ на простые множители.

6. Понятіе о простыхъ числахъ; число простыхъ чиселъ бесконечно....	8
7. Основныя свойства простыхъ чиселъ....	9

### § III. Условія дѣлимости. Слѣдствія.

8. Условія дѣлимости. Число дѣлителей; ихъ сумма.....	10
9. Наибольшая степень $p^m$ , дѣлящая произведеніе $1.2...n$ .....	13
10. Выводъ одной формулы.....	17
11. Число чиселъ, простыхъ съ $a$ и не превышающихъ $a$ .....	24
12—13. Свойства функціи $\varphi(a)$ .....	29
14. Рѣшеніе одной задачи.....	35
15. Примѣры.....	39

## ГЛАВА II.

Рѣшеніе въ цѣлыхъ числахъ нѣсколькихъ неопредѣленныхъ задачъ.

## § I. Общее рѣшеніе линейнаго однороднаго уравненія.

стр.

16. Выводъ теоремы.....	42
17. Приложение къ частному примѣру.....	45

## § II. Составленіе опредѣлителя, значеніе котораго равно 1, при данныхъ элементахъ первой строки.

18. Предварительныя замѣчанія.....	47
19. Способъ рѣшенія задачи.....	49
20. Примѣръ.....	51

## § III. Составленіе опредѣлителя при другихъ условіяхъ.

21. Предварительныя замѣчанія и способъ рѣшенія задачи.....	52
22. Примѣръ.....	55

## § IV. Новое рѣшеніе предыдущей задачи въ частномъ случаѣ, когда опредѣлитель 4-го порядка.

23. Рѣшеніе вспомогательной задачи.....	56
24. Рѣшеніе главнаго вопроса.....	60

## ГЛАВА III.

Понятіе о сравненіяхъ. — Сравненія первой степени.

## § I. О сравненіяхъ вообще.

25. Общія свойства сравненій.....	64
-----------------------------------	----

## § II. О наименьшихъ вычетахъ.

26. Опредѣленіе наименьшихъ вычетовъ.....	70
27. Абсолютно малый вычетъ.....	71
28. Доказательство одного предложенія.....	73
29. Распределеніе чиселъ на классы.....	74

## § III. Теорема Фермата.

30. Первое доказательство.....	75
31. Второе доказательство.....	78
32. Теорема Эйлера.....	79

### § IV. Слѣдствія изъ теоремы Фермата.

	стр.
33. Первое слѣдствіе изъ теоремы Фермата. Символь Лежандра.....	81
34. Теорема Вильсона.....	83
35. Всякое простое число вида $4n + 1$ разлагается на сумму двухъ квадратовъ .....	91
36. Новое доказательство теоремы Вильсона.....	96

### § V. Рѣшеніе сравненій первой степени.

37. Общія замѣчанія.....	98
38. Доказательство основной теоремы .....	99
39. Число рѣшеній какого угодно сравненія первой степени.....	102
40. Рѣшеніе нѣсколькихъ совокупныхъ сравненій первой степени съ различными модулями. ....	104
41. Частный случай. Примѣръ. ....	106
42. Сравненіе съ модулемъ сложнымъ приводится къ нѣсколькимъ сравненіямъ, модули которыхъ суть степени простыхъ чиселъ .....	107

### § VI. Рѣшеніе совокупныхъ сравненій съ нѣсколькими неизвѣстными.

43. Приведеніе къ простѣйшему виду .....	110
44. Случай, когда опредѣлитель системы и модуль взаимно простые. Примѣръ.....	113

## ГЛАВА IV.

Сравненія 2-ой степени. — Законъ взаимности простыхъ чиселъ.

### § I. Приведеніе сравненія къ простѣйшему виду. Условіе рѣшимости при модуль простомъ.

45. Простѣйшая форма сравненій второй степени.....	116
46. Число рѣшеній.....	118
47. Условіе возможности сравненія .....	119

### § II. Символь Лежандра.

48. Основные свойства символа Лежандра.....	121
49. Приведеніе символа Лежандра .....	129
50—52. Доказательства закона взаимности.....	130

### § III. Символь Якоби.

53. Опредѣленіе символа Якоби.....	142
54. Свойства символа Якоби.....	145
55. Вычисленіе величины символа.....	151

**§ IV. Рѣшеніе сравненія второй степени въ двухъ частныхъ случаяхъ.**

	стр.
56. Случай, когда можно получить прямо рѣшеніе сравненія съ помощью теоремы Вильсона или теоремы Фермата.....	153

**ГЛАВА V.**

Квадратичные вычеты и невычеты. — О дѣлителяхъ формы  $t^2 - Du^2$ .

**§ I. О квадратичныхъ вычетахъ.**

57. Опредѣленіе квадратичнаго вычета и нѣкоторыя его свойства.....	155
58. Квадратичные вычеты при сложномъ модуль.....	157
59. О корняхъ уравненія $\left(\frac{x}{p}\right) = \pm 1$ .....	158

**§ II. О рѣшеніяхъ уравненія  $\left(\frac{D}{x}\right) = \pm 1$ .**

60. Свойства выраженія $\left(\frac{D}{x}\right)$ .....	161
61. Число рѣшеній уравненія $\left(\frac{D}{x}\right) = \pm 1$ .....	165
62. О дѣлителяхъ формы $t^2 - Du^2$ .....	170

**ГЛАВА VI.**

Сравненіе второй степени при сложномъ модуль.

**§ I. Случай, когда модуль есть степень простаго числа.**

63. Случай, когда модуль есть степень простаго числа, приводится къ случаю, когда модуль есть число простое.....	173
64. Рѣшеніе сравненія $x^2 \equiv q \pmod{p^m}$ .....	176
65. Рѣшеніе сравненія $x^2 \equiv q \pmod{2^m}$ .....	178

**§ II. Число рѣшеній сравненія второй степени при сложномъ модуль. Слѣдствія.**

66. Число рѣшеній.....	184
67. Доказательство двухъ теоремъ.....	185

ГЛАВА VII.

О сравненіяхъ высшихъ степеней. — Двучленные сравненія.

§ I. Теорема Лагранжа.

	СТР.
68. Число корней сравненія не превышаетъ его степени.....	190

§ II. Разложеніе функцій на множители по данному модулю.

69. О функціяхъ, сравнимыхъ по модулю $p$ .....	193
70. Основныя дѣйствія надъ функціями по модулю $p$ .....	195
71. Доказательство одной теоремы.....	198
72. Общій наибольшій дѣлитель по модулю $p$ .....	200
73. О функціяхъ неприводимыхъ по модулю $p$ .....	203
74—75. Разложеніе функцій на неприводимые множители по модулю $p$ ...	204

§ III. Пониженіе степени сравненія.

76. Условія, чтобы сравненіе было возможно.....	213
77. Число рѣшеній какого угодно сравненія.....	214

§ IV. О двучленныхъ сравненіяхъ.

78. Условіе рѣшимости, необходимое и достаточное.....	216
-------------------------------------------------------	-----

ГЛАВА VIII.

Теорія первообразныхъ корней. — Свойства индексовъ.

§ I. О показателяхъ чиселъ по данному модулю.

79. Опредѣленіе показателя числа по данному модулю.....	221
80—82. Разныя свойства означеннаго показателя.....	226

§ II. О первообразныхъ корняхъ простыхъ чиселъ.

83. Доказательство существованія первообразнаго корня.....	231
84. Слѣдствія изъ предыдущаго.....	234
85. Таблица первообразныхъ корней.....	235

§ III. О первообразныхъ корняхъ чиселъ вида  $p^m$  или  $2p^m$ .

86. Распространеніе понятія о первообразныхъ корняхъ.....	235
87. О показательномъ сравненіи.....	236

	стр.
88—89. Доказательство существованія первообразныхъ корней. . . . .	237
90. Опредѣленіе наибольшаго показателя при модульѣ вида $2^m$ . . . . .	242
91—93. Слѣдствія, вытекающія изъ предыдущаго. . . . .	244

#### § IV. Опредѣленіе наибольшаго показателя при канонъ угодно модульѣ.

94. Доказательство вспомогательныхъ теоремъ. . . . .	246
95. Рѣшеніе вопроса о наибольшемъ показателѣ. . . . .	248
96. Пониженіе степени сравненія при сложномъ модульѣ. . . . .	249

#### § V. Обобщеніе теоремы Вильсона.

97. Доказательство одной леммы. . . . .	250
98. Теорема Вильсона въ обобщенной формѣ. . . . .	251

#### § VI. Теорія индексовъ.

99. Опредѣленіе индекса даннаго числа. . . . .	254
100—102. Свойства и употребленіе индексовъ. . . . .	255
103. Теорія индексовъ для модуля вида $2^m \geq 8$ . . . . .	261
104. Переходъ отъ одной системы индексовъ къ другой. . . . .	264

### ГЛАВА IX.

О функціональныхъ сравненіяхъ и неприводимыхъ функціяхъ.

#### § I. Сравненія съ двойнымъ модулемъ.

105. Опредѣленіе и основныя свойства сравненія съ двойнымъ модулемъ. . . . .	267
106. Теорема Фермата для функціональныхъ сравненій. . . . .	268
107. Функціональныя сравненія съ одной неизвѣстной. . . . .	270

#### § II. Теорема Лагранжа.

108. Теорема Лагранжа. . . . .	272
109—111. Слѣдствія изъ теоремъ Лагранжа и Фермата. . . . .	273

#### § III. Разложеніе функціи $x^{p^n} - x$ на неприводимые множители по модулю $p$ .

112. Доказательство основной теоремы. . . . .	278
113—116. Произведеніе всѣхъ неприводимыхъ функцій данной степени. . . . .	279
117. Число неприводимыхъ функцій данной степени. . . . .	285
118. Доказательство неприводимости одной функціи. . . . .	287

## § IV. О показателях функций по данному модулю.

	СТР.
119. Определѣніе показателя и характеристическія его свойства . . . . .	288

## § V. О надпоказателях функций по данному модулю.

120. Определѣніе надпоказателя и свойства его . . . . .	290
---------------------------------------------------------	-----

## § VI. Число функций, принадлежащих къ данному надпоказателю.

121. Искомое число дѣлится на данный надпоказатель . . . . .	294
122. Рѣшеніе вопроса . . . . .	296
123—124. Новый способ рѣшенія вопроса . . . . .	297
125. Составленіе неприводимыхъ функций данной степени . . . . .	303

## § VII. О порядкахъ неприводимыхъ функций.

126. Определѣніе порядка. Порядокъ опредѣляетъ собою степень . . . . .	304
127. Произведеніе всѣхъ функций $m$ -го порядка . . . . .	306
128. Число функций $m$ -го порядка . . . . .	307
129. Разложеніе функции $\psi_m$ въ случаѣ, когда $m$ дѣлится на $p$ . . . . .	308
130. Примѣръ . . . . .	309

## ГЛАВА X.

## О функцияхъ абсолютно неприводимыхъ.

## § I. Начала дѣлимости.

131—132. Начальныя понятія . . . . .	313
133—137. Разложеніе функций на абсолютно неприводимые множители . . . . .	315

## § II. Доказательство одного сравненія.

138. Результаты сравнимыхъ функций сравнимы . . . . .	323
139. Теорема Шенемана . . . . .	325

§ III. Разложеніе функции  $x^m - 1$  на неприводимые множители.

140. Разложеніе функции $x^m - 1$ на произведеніе функций $\psi_d$ . . . . .	327
141—142. Свойства корней функции $\psi_d$ . . . . .	328
143. Доказательство Дедекинда неприводимости функции $\psi_m$ . . . . .	330

**§ IV. Новое доказательство неприводимости функции  $\psi_m$  при  $m$   
равно  $\phi$  степени простого числа.**

	стр.
144. Доказательство вспомогательной леммы . . . . .	332
145—146. Доказательство неприводимости функции $\psi_{p^a}$ . . . . .	333
147. Функция $x^4 + 1$ по всякому модулю разлагается на множители . . . . .	335

---