

П.Л. Чебышев

Теория сравнений

**Москва
«Книга по Требованию»**

УДК 93
ББК 63.3
П11

П11 **П.Л. Чебышев**
Теория сравнений / П.Л. Чебышев – М.: Книга по Требованию, 2021. – 297 с.

ISBN 978-5-518-10222-4

ISBN 978-5-518-10222-4

© 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

III

до сихъ поръ находимъ первообразные корни, испытывая различные числа, и теоремы, изложенныя мною во второмъ приращеніи, едва ли не первый опытъ находить первообразные корни безъ предварительныхъ испытаній.

Исслѣдованія Ейлера о дѣлителяхъ чиселъ вида $a^n \pm b^n$ положили начало теоріи сравненій двучленныхъ. Эти исслѣдованія мы находимъ во многихъ мемуарахъ Ейлера; изъ нихъ особеннаго вниманія заслуживаетъ мемуаръ: *Theoremata circa divisores numerorum*. Здѣсь онъ показываетъ, что возможность удовлетворить сравненію $x^n - a \equiv 0 \pmod{mn + 1}$, при $mn + 1$ простымъ числѣ, предполагаетъ дѣлимость $a^m - 1$ на это число, и доказываетъ обратное, предполагая m и n простыми между собою. За исключеніемъ лишняго ограниченія m и n простыми между собою, эти теоремы суть основанія современной теоріи сравненій двучленныхъ вообще и въ особенности теоріи квадратичныхъ вычетовъ. Впрочемъ разсматривая у Ейлера доказательство послѣдней теоремы, легко замѣтить распространеніе ея на случай m и n какихъ нибудь. Въ мемуарѣ: *De quibusdam eximiiis proprietatibus circa divisores potestatum occurrentibus* онъ особенно доказываетъ это для случая $m = 2$, не дѣлая никакихъ ограничешій относительно n , и показываетъ, что дѣлимость $a^n - 1$ на $2n + 1$ есть необходимое и достаточное условіе того, чтобы a было квадратичнымъ вычетомъ числа $2n + 1$. Кромѣ того Эйлеръ, въ другихъ мемуарахъ, много занимался квадратичными вычетами, и въ *Observationes circa divisionem quadratorum per numeros primos*, разсматривая остатки, получаемые при дѣленіи квадратовъ на простые числа, онъ вывелъ такое заключеніе:

IV

Existente s numero quocunque primo, dividantur tantum quadrata imparia 1, 9, 25, 49, etc. per divisorem 4s, notenturque residua, quae omnia erunt formae 4q + 1, quorum quodvis littera α indicetur, reliquorum autem numerorum, formae 4q + 1, qui inter residua non occurrunt, quilibet littera X indicetur, quo facto si fuerit

<i>divisor numerus</i>		
<i>primus formae</i>		<i>tum est</i>
$4ns + \alpha$		$+ s$ residuum et $- s$ residuum
$4ns - \alpha$		$+ s$ residuum et $- s$ non-residuum
$4ns + X$		$+ s$ non-residuum et $- s$ non-residuum
$4ns - X$		$+ s$ non-residuum et $- s$ residuum.

Это открытіе мы находимъ у Ейлера въ 1-мъ томѣ *Opera scula Analytica*, 1772 года. Не трудно въ немъ узнать законъ взаимности двухъ простыхъ чиселъ, обнародованный Лежандромъ въ 1785 годѣ и положенный имъ въ основаніе теоріи квадратичныхъ вычетовъ.

Въ теоріи квадратичныхъ формъ Эйлеръ началъ свои изысканія съ суммы двухъ квадратовъ, и въ мемуарѣ: *De numeris, qui sunt aggregata duorum quadratorum* доказалъ, что дѣлители суммы двухъ квадратовъ простыхъ между собою должны представлять подобную сумму, и вывелъ линейную форму этихъ дѣлителей. Такимъ образомъ онъ дошелъ до знаменитой теоремы Фермата о разложеніи простыхъ чиселъ вида $4m + 1$ на два квадрата. Подобнымъ образомъ Эйлеръ нашелъ квадратичныхъ и линейныхъ дѣлителей для квадрата, сложенного съ удвоеннымъ или утроеннымъ квадратомъ, и предложилъ безъ доказательства линейныя формы дѣлителей многихъ квадратич-

ныхъ формъ. Такъ положилъ Эйлеръ основаніе теоріи дѣлителей квадратичныхъ формъ. Геніальныя открытія, сдѣланныя Лагранжемъ въ этой части Теоріи чиселъ, открыли путь Эйлеру къ новымъ изысканіямъ. Слѣдствіемъ ихъ было новое развитіе теоріи квадратичныхъ формъ со многими приложениями ея къ изслѣдованію, что данное число простое или нѣтъ, и какъ можно найти простые числа чрезвычайно большія.

Эйлеръ не ограничивался въ изысканіяхъ своихъ одними конечными формулами; онъ показалъ также, какимъ образомъ употребленіемъ рядовъ можно дойти до различныхъ предложеній Теоріи чиселъ. Сюда относятся изысканія *ergo de partitione numerorum* и о суммахъ дѣлителей различныхъ чиселъ.

Имѣя въ виду развитіе общей части Теоріи чиселъ, мы будемъ останавливаться на изысканіяхъ Эйлера въ Анализѣ Диофанта, результатомъ которыхъ было рѣшеніе уравненій второй степени съ двумя неизвѣстными, изслѣдованіе уравненій вида $ax^2 + by^2 = cz^2$, доказательство невозможности нѣкоторыхъ уравненій съ двумя и тремя неизвѣстными и рѣшеніе многихъ неопредѣленныхъ уравненій весьма сложныхъ, и перейдемъ къ изысканіямъ Лагранжа, которымъ сдѣлашы весьма важныя развитія въ общихъ началахъ Теоріи чиселъ. Сюда относятся изысканія его о числѣ рѣшеній, допускаемыхъ сравненіями съ простымъ модулемъ, и изслѣдованія свойствъ квадратичныхъ формъ. Мы видѣли, что Эйлеромъ найденъ высшій предѣлъ числа рѣшеній двучленныхъ сравненій; Лагранжъ доказалъ, что этотъ же предѣлъ будетъ при всякомъ числѣ членовъ. Этимъ открытіемъ Лагранжъ далъ возможность доказать многія предложенія Теоріи чиселъ, которыхъ доказательства прежде представляли непреодолимые затрудненія. Къ числу такихъ предложеній должно отнести существованіе первообразныхъ корней для

всѣхъ простыхъ чиселъ; доказательство, предложенное на это Эйлеромъ, основывается на свойствахъ двучленныхъ сравненій, которое могло быть строго доказано только послѣ открытія Лагранжа. Но изъ всѣхъ трудовъ Лагранжа въ Теоріи чиселъ наиболѣе имѣлъ вліянія на успѣхъ этой науки его изысканія о квадратичныхъ формахъ. Онъ далъ общія начала для тѣхъ изысканій, которыя сдѣланы были Эйлеромъ для не многихъ простѣйшихъ формъ, и эти начала, развитыя Лежандромъ, составили полную теорію дѣлителей квадратичныхъ формъ, одну изъ самыхъ главныхъ въ Теоріи чиселъ и особенно важную по своимъ приложениямъ къ опредѣленію дѣлителей даннаго числа.

Развитіе теоріи квадратичныхъ формъ, сдѣланное Лежандромъ, было слѣдствіемъ открытій его въ теоріи квадратичныхъ вычетовъ. Заключение, приведенное нами выше изъ сочиненія Ейлера: *Observationes circa divisionem quadratorum per numeros primos* содержитъ ту теорему, которая нынѣ извѣстна подъ именемъ закона взаимности двухъ простыхъ чиселъ и которой обязана своимъ успѣхомъ теорія квадратичныхъ вычетовъ. Въ запискахъ Парижской Академіи наукъ за 1785 годъ Лежандръ доказалъ ее на основаніи признаковъ возможности уравненій $ax^2 + by^2 = cz^2$, имѣ же открытыхъ, и показалъ приложения ея къ изслѣдованію сравненій второй степени и опредѣленію дѣлителей квадратичныхъ формъ.

Въ такомъ состояніи находились различныя части Теоріи чиселъ, когда Лежандръ написалъ сочиненіе свое: *Essai sur la Théorie des nombres*, изданное послѣ со многими прибавленіями, но безъ существенныхъ измѣненій въ системѣ изложенія главныхъ частей, подъ названіемъ *Théorie des nombres*. При всемъ развитіи отдѣльныхъ частей Теоріи чиселъ, систематическое изложенеіе этой науки представляло непреодолимыя трудности.

VII

Мы видѣли, что законъ взаимности двухъ простыхъ чиселъ, служащій основаніемъ теоріи квадратичныхъ вычетовъ и вслѣдствіе того необходимый для теоріи квадратичныхъ формъ, выведенъ былъ Лежандромъ изъ свойствъ уравненій второй степени. Поэтому теорія квадратичныхъ вычетовъ и формъ могла быть изложена только послѣ предварительнаго изложенія теоріи неопредѣленныхъ уравненій второй степени, теоріи по предмету своему гораздо высшей и съ своей стороны представляющей приложеніе теоріи квадратичныхъ вычетовъ. Вслѣдствіе этого въ сочиненіи своемъ Лежандръ, послѣ предварительнаго изложенія различныхъ предложеній относительно чиселъ, начинаетъ съ рѣшенія неопредѣленныхъ уравненій, и только по изложеніи полной теоріи уравненій второй степени онъ приступаетъ къ *общимъ свойствамъ чиселъ*, гдѣ находимъ у него главныя предложенія Теоріи сравненій и полную теорію квадратичныхъ вычетовъ и квадратичныхъ формъ. Такой порядокъ въ изложеніи главныхъ частей Теоріи чиселъ, лишившій ее системы, оставался необходимымъ только до тѣхъ поръ, пока Гауссъ не показалъ, какимъ образомъ законъ взаимности двухъ простыхъ чиселъ можетъ быть выведенъ непосредственно изъ разсмотрѣнія сравненій. Такъ открылась возможность, не нарушая естественнаго порядка въ главныхъ частяхъ Теоріи чиселъ, изложить сравненія второй степени вмѣстѣ съ другими сравненіями прежде уравненій второй степени, и потомъ на основаніи результатовъ Теоріи сравненій упростить изслѣдованіе уравненій высшихъ степеней.

Обращаемся теперь къ сочиненію Гаусса. Мы видѣли, какія развитія сдѣланы были въ различныхъ частяхъ Теоріи чиселъ трудами Ейлера, Лагранжа и Лежандра. Но Гауссъ въ сочиненіи своемъ: *Disquisitiones arithmeticae* не пользовался изысканія-

VIII

ми этихъ Геометровъ. Онъ независимо отъ нихъ развилъ главныя части Теоріи чиселъ, обогативъ ее новыми приемами, многими отысканіями и весьма важными приложениями къ рѣшенію двузначныхъ уравненій. Но при всемъ достоинствѣ сочиненія Гаусса мы не можемъ не признать, что большая часть его выводовъ лишена той простоты, которою отличаются приемы Ейлера, Лагранжа и Лежандра. Въ этомъ отношеніи его изложеніе отдѣльныхъ частей Теоріи чиселъ, за исключеніемъ нѣкоторыхъ, нельзя предпочесть изложенію Лежандра.

Изъ этого видно, что ни сочиненіе Лежандра, ни сочиненіе Гаусса не представляютъ Теоріи чиселъ въ томъ совершенномъ видѣ, въ которомъ она можетъ быть изложена послѣ развитій, сдѣланныхъ въ ней трудами этихъ Геометровъ, а тѣмъ болѣе послѣ изысканій Геометровъ позднѣйшихъ. Поэтому въ изложеніи Теоріи сравненій я долженъ былъ руководствоваться не однимъ Лежандромъ и не однимъ Гауссомъ, но вмѣстѣ и Лежандромъ и Гауссомъ и многими другими, занимавшимися этою частью Теоріи чиселъ. Но чтобы привести въ систему изысканія Геометровъ, употреблявшихъ приемы весьма разнообразныя, я долженъ былъ измѣнить большую часть ихъ выводовъ. Кромѣ того для полноты системы я нашелъ необходимымъ развить нѣкоторыя статьи. Такъ въ теоріи сравненій f -й степени я рассматриваю отдѣльно три случая, когда это сравненіе имѣетъ одно рѣшеніе, нѣсколько и не имѣетъ ни одного. Излагая свойства сравненій высшихъ степеней, предлагаю относительно ихъ нѣсколько общихъ теоремъ, кромѣ теоремы Лагранжа. Въ теоріи квадратичныхъ формъ показываю средство узнавать, когда двѣ квадратичныя формы дѣлителей приводятся къ однимъ линейнымъ формамъ. Кромѣ того въ сочиненіи моемъ находятся три прибавленія. Въ первомъ я излагаю распростра-

IX

неніе знакоположенія Лежандра, сдѣланное Якоби, и показываю приложение этого къ изслѣдованію квадратичныхъ вычетовъ; во второмъ я доказываю теоремы, опредѣляющія первообразный корень нѣкоторыхъ чиселъ по ихъ виду; въ третьемъ я предлагаю результаты своихъ изысканій относительно свойствъ функціи, опредѣляющей сколько простыхъ чиселъ не превосходятъ данной величины.



ОГЛАВЛЕНИЕ.

ПРЕДВАРИТЕЛЬНЫЯ ПОНЯТІЯ.

§§.	Стран.
1. Предметъ Теоріи чиселъ и Теоріи сравненій.....	1
2. О числахъ абсолютно простыхъ.....	2
3. О числахъ относительно простыхъ.....	3
4. Свойства чиселъ относительно простыхъ.....	—
5. О разложеніи чиселъ на простые множители.....	5
6. Теоремы на этомъ основанія.....	7
7. О числахъ, составляющихъ арифметическую прогрессию.....	12

ГЛАВА I.

О сравненіи вообще.

8. Понятіе о сравненіи.....	18
9. О свойствахъ сравненія чиселъ между собою.....	19
10. О рѣшеніи сравненій.....	23
11. О наименьшихъ вычетахъ.....	24
12. О числѣ рѣшеній сравненія.....	27

ГЛАВА II.

О сравненіи первой степени.

13. Рѣшеніе этихъ сравненій при модуль простомъ съ коэффициентомъ неизвѣстнаго.....	30
14. Теоремы Фермата и Ейлера.....	31
15. Приложеніе этихъ теоремъ къ рѣшенію сравненій 1-й степени.....	35
16. О сравненіяхъ, въ которыхъ модуль и коэффициентъ неизвѣстнаго имѣютъ общаго дѣлителя.....	37

II

ГЛАВА III.

О сравненіяхъ высшихъ степеней вообще.

§§	страниц.
17. Освобожденіе отъ коэффициента высшей степени независимаго.....	40
18. Высшей предѣлъ числа рѣшеній.....	42
19. Приложеніе этого къ доказательству теоремы Вильсона и другихъ свойствъ чиселъ.....	45
20. Приведеніе сравненій къ виду, въ которомъ степень его меньше модуля.....	49
21. Признакъ, по которому узнаемъ, что сравненіе имѣетъ столько рѣшеній, сколько единицъ въ показателѣ его.....	50

ГЛАВА IV.

О сравненіяхъ второй степени.

22. Приведеніе полныхъ сравненій второй степени къ сравненію вида $z^2 \equiv q \pmod{p}$	54
23. О числѣ рѣшеній сравненія $z^2 \equiv q \pmod{p}$	58
24. О символѣ $\left(\frac{q}{p}\right)$	59
25. Свойства этого символа.....	61
26. Выраженія его опредѣляющія; следствія ихъ: 1) значеніе $\left(\frac{2}{p}\right)$, 2) законъ взаимности двухъ простыхъ чиселъ.....	64
27. Способъ находить значеніе $\left(\frac{q}{p}\right)$	78
28. Рѣшеніе уравненій: $\left(\frac{x}{p}\right) = 1$, $\left(\frac{x}{p}\right) = -1$	81
29. Рѣшенія сравненія $z^2 \equiv q \pmod{p}$, при p простомъ вида $4n + 3$...	85
30. О сравненіяхъ $z^2 \equiv q \pmod{p}$ при p составномъ.....	86

ГЛАВА V.

О сравненіяхъ двучленныхъ.

31. О сравненіяхъ $x^m + A \equiv 0 \pmod{p}$, при p простомъ.....	91
32. О сравненіяхъ $x^m + A \equiv 0 \pmod{p}$ при p простомъ.....	96
33. О сравненіяхъ $x^m + A \equiv 0 \pmod{p}$ при p составномъ.....	102