П.Л. Чебышев

Теория сравнений

Москва
«Книга по Требованию»

УДК 93
ББК 63.3
П11

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

ISBN 978-5-518-10222-4

ISBN 978-5-518-10222-4

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

Изслѣдованія Ейлера о дѣлителяхъ чиселъ вида $a^n \pm b^n$ положили начало теоріи сравненій двучленныхъ. Эти изслѣдованія мы находимъ во многихъ мемуарахъ Ейлера; изъ нихъ особеннаго вниманія заслуживаетъ мемуаръ: *Theoremata circa divisores numerorum.* Здѣсь онъ показываетъ, что возможность удовлетворить сравненію $x^n - a \equiv 0$ (*мод.* $mn + 1$), при $mn + 1$ простомъ 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 eximiis proprietatibus circa divisores potestatum occurentibus* онъ особенно доказываетъ это для случая $m = 2$, не дѣлая никакихъ ограниченій 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 Ейлеръ, въ другихъ мемуарахъ, много занимался квадратичными вычетами, и въ *Observationes circa divisionem quadratorum per numeros primos*, разсматривая остатки, получаемые при дѣленіи квадратовъ на простыя числа, онъ вывелъ такое заключеніе:

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 occurunt, quilibet littera* $\mathfrak{A}$ *indicetur, quo facto si fuerit*

divisor numerus primus formae	*tum est*
$4ns + \alpha$	$+ s$ *residuum et* $- s$ *residuum*
$4ns - \alpha$	$+ s$ *residuum et* $- s$ *non-residuum*
$4ns + \mathfrak{A}$	$+ s$ *non-residuum et* $- s$ *non-residuum*
$4ns - \mathfrak{A}$	$+ s$ *non-residuum et* $- s$ *residuum.*

Это открытіе мы находимъ у Ейлера въ 1-мъ томѣ Opuscula 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 Ейлеръ 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 Ейлеръ нашелъ квадратичныхъ и линейныхъ дѣлителей для квадрата, сложеннаго съ удвоеннымъ или утроеннымъ квадратомъ, и предложилъ безъ доказательства линейныя формы дѣлителей многихъ квадратич-

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

Ейлеръ 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 его *de partitione numerorum* и о суммахъ дѣлителей различныхъ чиселъ.

Имѣя въ виду развитіе общей части Теоріи чиселъ, мы не будемъ останавливаться на изысканіяхъ Ейлера въ Анализѣ Діофанта, результатомъ которыхъ было рѣшеніе уравненій второй отепени 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 сдѣланы 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 Ейлеромъ 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 непреодолимыя затрудненія. Къ числу такихъ предложеній должно отнести существованіе первообразныхъ корней для

всѣхъ простыхъ чиселъ; доказательство, предложенное на это Эйлеромъ, основывается на свойствѣ двучленныхъ сравненій, которое могло быть строго доказано только послѣ открытія Лагранжа. Но изъ всѣхъ трудовъ Лагранжа въ Теоріи чиселъ наиболѣе имѣли 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 приложеніямъ къ опредѣленію дѣлителей даннаго числа.

Развитіе теоріи квадратичныхъ формъ, сдѣланное Лежандромъ, было слѣдствіемъ открытій его въ теоріи квадратичныхъ вычетовъ. Заключеніе, приведенное нами выше изъ сочиненія Эйлера: *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 уравненія $ax^2 + by^2 = cz^2$, имъ же открытыхъ, и показалъ приложенія 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 изложеніе этой науки представляло непреодолимыя трудности.

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 разсматриванія 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-

ми этихъ Геометровъ. Онъ независимо отъ нихъ развилъ главныя части Теоріи чиселъ, обогативъ ее новыми пріемами, многими открытіями и весьма важными приложеніями къ рѣшенію двучленныхъ уравненій. Но при всемъ достоинствѣ сочиненія Гаусса мы не можемъ не признать, что большая часть его выводовъ лишена той простоты, которою отличаются пріемы Эйлера, 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 пріемы весьма разнообразные, я долженъ былъ измѣнить большую часть ихъ выводовъ. Кромѣ того для полноты системы я нашелъ необходимымъ развить нѣкоторыя статьи. Такъ въ теоріи сравненій 1-й степени я разсматриваю 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-

неніе знакоположенія Лежандра, сдѣланное Якоби, и показываю приложеніе 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.

ОГЛАВЛЕНІЕ.

ПРЕДВАРИТЕЛЬНЫЯ ПОНЯТІЯ.

ГЛАВА I.

О сравненіи вообще.

ГЛАВА II.

О сравненіи первой степени.

II

ГЛАВА III.

О сравненіяхъ высшихъ степеней вообще.

ГЛАВА IV.

О сравненіяхъ второй степени.

ГЛАВА V.

О сравненіяхъ двучленныхъ.