П. Я. Москальскій.

Доказательство великаго предложенія Фермата

„. . . Невозможно разложить полный кубъ на сумму двухъ кубовъ, четвертую степень на сумму двухъ четвертыхъ степеней, вообще, какую-либо степень на сумму двухъ степеней съ тѣмъ же показателемъ, если послѣдній больше двухъ".

П. Ферматъ.

Юрьевъ.
Типографія Эд. Бергмана.
1910.

П. Я. Москальскій.

Доказательство великаго предложенія Ферматa

„ . . . Невозможно разложить полный кубъ на сумму двухъ кубовъ, четвертую степень на сумму двухъ четвертыхъ степеней, вообще, какую-либо степень на сумму двухъ степеней съ тѣмъ же показателемъ, если послѣдній больше двухъ“.

П. Ферматъ.

Юрьевъ.
Типографія Эд. Бергмана.
1910.

Вступленіе.

Пьеръ Ферматъ, авторъ той теоремы, которую я доказываю ниже, жилъ отъ 1601 по 1665 г.

Онъ былъ юристомъ и занимался математикой между прочимъ. Это не помѣшало Фермату сдѣлать много интересныхъ открытій въ области математическихъ наукъ. Особенною любовью его пользовалась теорія чиселъ, въ его время совершенно неразработанная наука. Своими открытіями въ этой области Ферматъ по праву заслужилъ званіе великаго геометра.

Труды свои Пьеръ Ферматъ нигдѣ не печаталъ, а въ лучшемъ случаѣ сообщалъ въ письмахъ своимъ друзьямъ. Многія предложенія Ферматъ оставилъ безъ доказательствъ. Позже математики доказали всѣ предложенія Фермата, кромѣ одного.

На поляхъ сочиненія Діафанта противъ того мѣста, гдѣ послѣдній трактуетъ о разложеніи полнаго квадрата на сумму двухъ квадратовъ, Пьеръ Ферматъ написалъ слѣдующее:

„Между тѣмъ совершенно невозможно разложить полный кубъ на сумму двухъ кубовъ, четвертую степень на сумму двухъ четвертыхъ степеней, вообще, какую-либо степень на сумму двухъ степеней съ тѣмъ же показателемъ, если послѣдній больше двухъ. Я нашелъ поистинѣ удивительное доказательство этого предложенія, но здѣсь слишкомъ мало мѣста, чтобы его помѣстить.“

Такъ это доказательство и осталось неизвѣстнымъ. Позднѣйшіе математики много трудились надъ этой теоремой, но всѣ ихъ попытки не увѣнчались успѣхомъ. Замѣтимъ между прочимъ, что Эйлеръ доказалъ теорему для 4-ой степени. Больше другихъ сдѣлалъ Куммеръ. Онъ доказалъ теорему для всякаго простого показателя, кромѣ 37, 59 и 67. Такимъ образомъ, до сихъ поръ еще никому не удалось найти общее доказательство великаго предложенія Фермата.

Зная это, я все же беру на себя смѣлость выпустить свой трудъ съ надеждою, что мною открыта истина.

Доказательство, благодаря его сложности, я предпочелъ раздѣлить на двѣ части и вести въ видѣ отдѣльныхъ теоремъ, изъ которыхъ, какъ слѣдствіе, вытекаетъ предложеніе Фермата. Въ первой части я докажу

нѣкоторыя свойства чиселъ, которыя не встрѣчаются въ современныхъ трудахъ по теоріи чиселъ. Во второй части я вывожу тѣ свойства уравненія $x^n + y^n = z^n$,

на основаніи которыхъ доказывается предложеніе Фермата.

Я умышленно нѣсколько усложняю доказательство, чтобы показать, что Пьеръ Ферматъ могъ доказать великое предложеніе, предполагая, что мое доказательство вѣрно. Дѣлаю это съ тою цѣлью, чтобы опровергнуть мнѣніе многихъ математиковъ, что Ферматъ высказалъ свое предложеніе, не имѣя достаточно обоснованнаго доказательства, такъ какъ онъ, по предположенію тѣхъ же математиковъ, не имѣлъ данныхъ, чтобы доказать великое предложеніе.

Взявъ на себя такую задачу, я не могъ пользоваться тѣмъ что было открыто послѣ Фермата. Главнымъ образомъ это относится къ биному Ньютона и теоремѣ Эйлера:

$$a^{\varphi(N)} \equiv 1 \ (Mod\ N),$$

а потому въ доказательствѣ я укажу тѣ мѣста, гдѣ ими можно пользоваться. Нужно, однако, замѣтить, что изъ этого условія я исключаю доказательство Эйлера при $n = 4$ предложенія Фермата, такъ какъ это доказательство основано на такихъ истинахъ, которыя Ферматъ безъ сомнѣнія зналъ.

Приступая къ доказательству, я предполагаю, что читатель знакомъ съ основными свойствами чиселъ и сравненій, а потому пользуюсь ими безъ доказательствъ. Кромѣ того, я позволю себѣ поставить нѣкоторыя условія относительно терминовъ и значеній буквъ, чтобы избѣжать какихъ бы то ни было недоразумѣній.

Во первыхъ, числа, дѣлящіяся только на самихъ себя и единицу, я называю простыми, а два или нѣсколько чиселъ, которыя не имѣютъ общихъ дѣлителей больше единицы, я называю взаимно простыми.

Во вторыхъ, показатели степеней и модули въ сравненіяхъ я всегда предполагаю числами цѣлыми и положительными. Подъ всѣми другими буквами, кромѣ x, y и z, я всегда подразумѣваю числа цѣлыя, положительныя или отрицательныя, не равныя нулю, который обозначаю общепринятымъ знакомъ.

Каждый разъ, когда нужно будетъ измѣнить этимъ условіямъ, я буду указывать въ текстѣ на характеръ такого измѣненія.

17 (30) сент. 1910 г.

П. Москальскій.

Часть I.

Нѣкоторыя свойства чиселъ.

Теорема I. Если имѣемъ сравненіе

$$A^n - B^n \equiv O\ (Mod\ n) \tag{1}$$

гдѣ n — число простое, то $A - B \equiv O\ (Mod\ n)$

Доказательство. Каковы бы ни были числа A и B, сравненія:

$$A^n \equiv A\ (Mod\ n) \tag{2}$$

$$B^n \equiv B\ (Mod\ n) \tag{3}$$

всегда возможны. Вычитая (3) изъ (2), получимъ:

$$A^n - B^n \equiv A - B\ (Mod\ n) \tag{4}$$

Изъ (4), принявъ во вниманіе (1), найдемъ:

$$A - B \equiv O\ (Mod\ n)$$

Что и требовалось доказать.

Теорема II. Если имѣемъ сравненіе:

$$A^n + B^n \equiv O\ (Mod\ n) \tag{5}$$

гдѣ n число простое, то $A + B \equiv O\ (Mod\ n)$

Доказательство. Снова имѣемъ право написать сравненія:

$$A^n \equiv A\ (Mod\ n) \tag{6}$$

$$B^n \equiv B\ (Mod\ n) \tag{7}$$

Складывая (6) съ (7), получимъ:

$$A^n + B^n \equiv A + B\ (Mod\ n) \tag{8}$$

Изъ (8), принявъ во вниманіе (5), найдемъ:

$$A + B \equiv O\ (Mod\ n)$$

Что и требовалось.

Теорема III. $A-B$ и частное отъ дѣленія $A^n - B^n$ на $A-B$ не могутъ имѣть общихъ множителей большихъ единицы и взаимно простыхъ съ n, если A и B числа взаимно простыя.

Доказательство. Допустимъ противное. Пусть

$$A - B \equiv O\ (Mod\ r) \tag{9}$$

и

$$S \equiv O\ (Mod\ r) \tag{10}$$

гдѣ $S = \frac{A^n - B^n}{A - B} = A^{n-1} + A^{n-2}B + A^{n-3}B^2 + \ldots\ldots +$

$$+ AB^{n-2} + B^{n-1} = (A - B)\left[A^{n-2} + 2A^{n-3}B + 3A^{n-4}B^2 + \right.$$

$$\left. + \ldots\ldots + (n-2)AB^{n-3} + (n-1)B^{n-2}\right] + nB^{n-1} \tag{11}$$

Равенство (11) мы получимъ, если раздѣлимъ $A^n - B^n$ на $A-B$; полученное частное еще разъ дѣлимъ на $A-B$ и приравниваемъ дѣлимое произведенію дѣлителя на частное и затѣмъ прибавимъ остатокъ. Подъ r въ сравненіяхъ (9) и (10) будемъ разумѣть число большее единицы, взаимно простое съ n и простое само по себѣ. Подставимъ значеніе S изъ равенства (11) въ сравненіе (10)

$$(A - B)\left[A^{n-2} + 2A^{n-3}B + 3A^{n-4}B^2 + \ldots\ldots + (n-2)AB^{n-3} + \right.$$

$$\left. + (n-1)B^{n-2}\right] + nB^{n-1} \equiv O\ (Mod\ r) \tag{12}$$

Принявъ во вниманіе сравненіе (9), найдемъ, что первый членъ лѣвой части сравненія (12) дѣлится на r, такъ какъ дѣлится на $A-B$, а потому на r долженъ дѣлиться и второй членъ.

Слѣдовательно: $$nB^{n-1} \equiv O\ (Mod\ r) \tag{13}$$

Или, сокращая (13) на n, получимъ:

$$B^{n-1} \equiv O\ (Mod\ r) \tag{14}$$

Такъ какъ r по условію число простое, то сравненіе (14) возможно только тогда, когда

$$B \equiv O\ (Mod\ r) \tag{15}$$

а въ такомъ случаѣ изъ (9) и (15) имѣемъ:

$$A \equiv O\ (Mod\ r) \tag{16}$$

Сравненія (15) и (16) противорѣчатъ условію, что A и B числа взаимно простыя. Изъ этого вытекаетъ, что наше допущеніе е имѣетъ мѣста, и теорема доказана.

Теорема IV. $A + B$ и частное отъ дѣленія $A^n - B^n$ на $A + B$ не могутъ имѣть общихъ множителей больше единицы взаимно простыхъ съ n, если A и B числа взаимно простыя, и n — исло нечетное.

Доказательство. Допустимъ противное. Пусть

$$A + B \equiv O\ (Mod\ r) \tag{17}$$

$$T \equiv O\ (Mod\ r) \tag{18}$$

гдѣ $T=\frac{A^n+B^n}{A+B}=A^{n-1}-A^{n-2}B+A^{n-3}B^2-\ldots\ldots-AB^{n-2}+$

$+B^{n-1}=(A+B)[A^{n-2}-2A^{n-3}B+3A^{n-4}B^2-\ldots\ldots+$

$+(n-2)AB^{n-3}-(n-1)B^{n-2}]+nB^{n-1}$ (19)

Равенство (19) получимъ, если раздѣлимъ A^n+B^n на $A+B$ при n нечетномъ; полученное частное еще разъ дѣлимъ на $A+B$ и приравниваемъ дѣлимое произведенію дѣлителя на новое частное и затѣмъ прибавимъ остатокъ. Подъ r въ сравненіяхъ (17) и (18) подразумѣваемъ число большее единицы, взаимно простое съ n и простое само по себѣ. Подставивъ значеніе T изъ равенства (19) въ сравненіе (18), получимъ:

$(A+B)[A^{n-2}-2A^{n-3}B+3A^{n-4}B^2-\ldots\ldots+(n-2)AB^{n-3}-$

$-(n-1)B^{n-2}]+nB^{n-1}\equiv O\,(Mod\ r)$ (20)

Принявъ во вниманіе сравненіе (17), найдемъ, что первый членъ лѣвой части сравненія (20) дѣлится на r, а потому должны имѣть:

$$nB^{n-1}\equiv O\,(Mod\ r) \quad (21)$$

Сокративъ (21) на n, получимъ:

$$B^{n-1}\equiv O\,(Mod\ r) \quad (22)$$

Такъ какъ r по условію число простое, то изъ сравненія (22) вытекаетъ, что $B\equiv O\,(Mod\ r)$ (23)

а въ такомъ случаѣ изъ сравненій (17) и (23) имѣемъ:

$$A\equiv O\,(Mod\ r) \quad (24)$$

Сравненія (23) и (24) противорѣчатъ условію, что A и B числа взаимно простыя, а потому наше допущеніе невозможно, и теорема доказана.

Слѣдствіе. Какъ слѣдствіе изъ теоремъ III и IV вытекаетъ то, что S съ $A-B$ при n простомъ и T съ $A+B$ при n простомъ и нечетномъ не могутъ имѣть общихъ дѣлителей отличныхъ отъ n и единицы.

Теорема V. Если A^n-B^n дѣлится на n, гдѣ n — число простое, то: 1) частное отъ дѣленія A^n-B^n на $A-B$ дѣлится на n; 2) но это частное не можетъ дѣлиться на n^2, если A и B — числа взаимно простыя, а n число простое и нечетное.

Доказательство. Согласно теоремѣ I при нашихъ условіяхъ имѣемъ сравненіе: $A-B\equiv O\,(Mod\ n)$ (25)

Докажемъ первое, что

$$S\equiv O\,(Mod\ n) \quad (26)$$

гдѣ S — частное отъ дѣленія A^n-B^n на $A-B$. Замѣнивъ въ (26) S его значеніемъ изъ равенства (11), получимъ:

$(A-B)[A^{n-2}+2A^{n-3}B+3A^{n-4}B^2+\ldots\ldots+(n-2)AB^{n-3}+$

$+(n-1)B^{n-2}]+nB^{n-1}\equiv O\,(Mod\ n)$ (27)

Справедливость этого сравненія очевидна, если принять во вниманіе сравненіе (25). Въ самомъ дѣлѣ: первый членъ лѣвой части срав-

ненія (27) дѣлится на $A - B$, а потому дѣлится и на n, и второй членъ очевидно дѣлится на n.

Для доказательства второй части теоремы, допустимъ что

$$S \equiv O \ (Mod\ n^2) \tag{28}$$

Если въ правой части равенства (11) многочленъ, стоящій въ квадратныхъ скобкахъ, раздѣлимъ на $A-B$ и частное для краткости обозначимъ черезъ P, то получимъ:

$$S = (A - B)\left[(A - B)\,P + \frac{n\,(n-1)}{2} B^{n-2}\right] + n\,B^{n-1} =$$

$$= (A - B)^2 P + \frac{n\,(n-1)}{2}(A - B)\,B^{n-2} + n\,B^{n-1} \tag{29}$$

Изъ равенства (29) и сравненія (28) получимъ:

$$(A - B)^2 P + \frac{n\,(n-1)}{2}(A - B)\,B^{n-2} + n\,B^{n-1} \equiv O\ (Mod\ n^2) \tag{30}$$

Такъ какъ сравненіе (25) указываетъ на дѣлимость $A - B$ на n, то $(A - B)^2$ раздѣлится на n^2, а потому

$$(A - B)^2\ P \equiv O\ (Mod\ n^2) \tag{31}$$

Такъ же при дѣлимости $A - B$ на n и

$$\frac{n\,(n-1)}{2}(A - B)\,B^{n-2} \equiv O\ (Mod\ n^2) \tag{32}$$

такъ какъ n по условію число нечетное, а потому на 2 раздѣлится $n-1$. Изъ сравненій (30), (31) и (32) найдемъ:

$$n\,B^{n-1} \equiv O\ (Mod\ n^2)$$

которое, по сокращеніи числа и модуля на n, принимаетъ видъ:

$$B^{n-1} \equiv O\ (Mod\ n) \tag{33}$$

Такъ какъ n — число простое, то сравненіе (33) возможно только тогда, когда

$$B \equiv O\ (Mod\ n) \tag{34}$$

Изъ сравненій (25) и (34) имѣемъ:

$$A \equiv O\ (Mod\ n) \tag{35}$$

Сравненія (34) и (35) доказываютъ, что наше допущеніе невозможно, такъ какъ по условію A и B числа взаимно простыя. Этимъ и доказывается предложенная теорема.

Теорема VI. Если $A^n + B^n$ дѣлится на n, то и частное отъ дѣленія $A^n + B^n$ на $A + B$ дѣлится на n, но не можетъ дѣлиться на n^2, когда A и B числа взаимно простыя; n — число простое и нечетное.

Доказательство. При нашихъ условіяхъ по теоремѣ II имѣемъ:

$$A + B \equiv O\ (Mod\ n) \tag{36}$$

Докажемъ во первыхъ, что

$$T \equiv O\ (Mod\ n) \tag{37}$$

гдѣ T — частное отъ дѣленія $A^n + B^n$ на $A + B$. Замѣнимъ T его значеніемъ изъ равенства (19):

$$(A+B)\,[A^{n-2} - 2\,A^{n-3}\,B + 3\,A^{n-4}\,B^2 - \ldots\ldots + (n-2)\,A\,B^{n-3} - \\ - (n-1)\,B^{n-2}] + n\,B^{n-1} \equiv O\,(Mod\ n) \qquad (38)$$

Справедливость сравненія (38) очевидна, если принять во вниманіе сравненіе (36), такъ какъ при этомъ первый членъ лѣвой части дѣлится на n, а второй очевидно дѣлится на n.

Для доказательства второй части теоремы допустимъ, что

$$T \equiv O\,(Mod\ n^2) \qquad (39)$$

Если въ правой части равенства (19) многочленъ, заключенный въ квадратныя скобки, раздѣлимъ на $A + B$ и частное обозначимъ черезъ R, то получимъ:

$$T = (A+B)\left[(A+B)\,R - \frac{n(n-1)}{2}\,B^{n-2}\right] + n\,B^{n-1} = \\ = (A+B)^2\,R - \frac{n(n-1)}{2}\,(A+B)\,B^{n-2} + n\,B^{n-1} \qquad (40)$$

Изъ равенства (40) и сравненія (39) имѣемъ:

$$(A+B)^2\,R - \frac{n(n-1)}{2}\,(A+B)\,B^{n-2} + n\,B^{n-1} \equiv O\,(Mod\ n^2) \qquad (41)$$

Такъ какъ сравненіе (36) указываетъ на дѣлимость $A + B$ на n, то $(A+B)^2$ раздѣлится на n^2, и слѣдовательно:

$$(A+B)^2\,R \equiv O\,(Mod\ n^2) \qquad (42)$$

Такъ же при дѣлимости $A + B$ на n и

$$\frac{n(n-1)}{2}\,(A+B)\,B^{n-2} \equiv O\,(Mod\ n^2) \qquad (43)$$

такъ какъ n по условію число нечетное, а потому на 2 раздѣлится $n - 1$. Изъ сравненій (41), (42) и (43) найдемъ:

$$n\,B^{n-1} \equiv O\,(Mod\ n^2) \qquad (44)$$

Сокращая въ (44) на n число и модуль, получимъ:

$$B^{n-1} \equiv O\,(Mod\ n)$$

Такъ какъ n число простое, то послѣднее сравненіе возможно только тогда, когда

$$B \equiv O\,(Mod\ n) \qquad (45)$$

Изъ сравненій (36) и (45) находимъ:

$$A \equiv O\,(Mod\ n) \qquad (46)$$

Сравненія (45) и (46) противорѣчатъ условію, что A и B числа взаимно простыя, а потому наше допущеніе невозможно и теорема доказана.

Примѣчаніе. При доказательствѣ теоремъ III, IV, V и VI можно воспользоваться биномомъ Ньютона. Имѣемъ:

$$A^n = [(A-B)+B]^n = (A-B)^n + n(A-B)^{n-1}B +$$
$$+\frac{n(n-1)}{1.2}(A-B)^{n-2}B^2 + \ldots\ldots + \frac{n(n-1)}{1.2}(A-B)^2 B^{n-2} +$$
$$+ n(A-B)B^{n-1} + B^n$$

Откуда легко получить:

$$A^n - B^n = (A-B)^n + n(A-B)^{n-1}B + \ldots\ldots +$$
$$+\frac{n(n-1)}{1.2}(A-B)^2 B^{n-2} + n(A-B)B^{n-1}$$

Точно такъ же при n нечетномъ: $A^n = [(A+B)-B]^n$, откуда

$$A^n + B^n = (A+B)^n - n(A+B)^{n-1}B + \frac{n(n-1)}{1.2}(A+B)^{n-2}B^2 -$$
$$- \ldots\ldots - \frac{n(n-1)}{1.2}(A+B)^2 B^{n-2} + n(A+B)B^{n-1}$$

Полученныя тождества не трудно примѣнить къ доказательству указанныхъ теоремъ. Они удобны тѣмъ, что при ихъ помощи легко находятся послѣдовательныя остатки при дѣленіи $A^n - B^n$ на $A-B$ и $A^n + B^n$ на $A+B$.

Теорема VII. Если возможно сравненіе:

$$A^n - B^n \equiv O\ (Mod\ n^q) \qquad (47)$$

гдѣ A и B числа взаимно простыя, а n — число простое, нечетное и больше единицы, то при $q > 1$

$$A - B \equiv O\ (Mod\ n^{q-1})$$

Доказательство. Въ (47) подставимъ вмѣсто дѣлимаго $A^n - B^n$ произведеніе дѣлителя $A-B$ на частное S. Имѣемъ:

$$(A-B)S \equiv O\ (Mod\ n^q) \qquad (48)$$

Согласно теоремѣ V S дѣлится на n, но не можетъ дѣлиться на n^2, а потому и въ высшихъ степеняхъ, слѣдовательно можемъ написать:

$$S = nM \qquad (49)$$

гдѣ M на n не дѣлится. Подставивъ значеніе S изъ (49) въ (48) и сокращая послѣднее на M, получимъ:

$$(A-B)n \equiv O\ (Mod\ n^q) \qquad (50)$$

Сокративъ въ (50) число и модуль на n, найдемъ:

$$A - B \equiv O\ (Mod\ n^{q-1})$$

Что и требовалось доказать.

Теорема VIII. Если возможно сравненіе

$$A^n + B^n \equiv O\ (Mod\ n^q) \qquad (51)$$

гдѣ A и B числа взаимно простыя, а n — число простое, нечетное и больше единицы, то при $q > 1$

$$A + B \equiv O \ (Mod\ n^{q-1})$$

Доказательство. Въ (51) подставимъ вмѣсто дѣлимаго $A^n + B^n$ произведеніе дѣлителя $A + B$ на частное T. Имѣемъ:

$$(A + B)\, T \equiv O \ (Mod\ n^q) \qquad (52)$$

По теоремѣ VI T дѣлится на n, но не можетъ дѣлиться на n^2, а слѣдовательно и въ высшихъ степеняхъ, а потому можемъ написать:

$$T = nQ \qquad (53)$$

гдѣ Q на n не дѣлится. Подставивъ значеніе T изъ (53) въ (52) и сокративъ послѣднее на Q, получимъ:

$$(A + B)\, n \equiv O \ (Mod\ n^q) \qquad (54)$$

Сокративъ въ (54) число и модуль на n, найдемъ:

$$A + B \equiv O \ (Mod\ n^{q-1})$$

Что и требовалось доказать.

Теорема IX. Если существуетъ сравненіе

$$A \equiv B \ (Mod\ n^s), \text{ или } A - B \equiv O \ (Mod\ n^s) \qquad (55)$$

то $A^{n^t} \equiv B^{n^t} \ (Mod\ n^{s+t})$, т. е. $A^{n^t} - B^{n^t} \equiv O \ (Mod\ n^{s+t})$ (56)

гдѣ n — число простое.

Доказательство. Докажемъ сначала, что эта теорема справедлива при t равномъ единицѣ. Согласно сравненію (55) $A - B$ дѣлится на n^s, а потому и $A^n - B^n$, какъ дѣлящееся на $A - B$, что видно изъ равенства (11), раздѣлится на n^s. При такихъ условіяхъ по теоремѣ V найдемъ, что частное S отъ дѣленія $A^n - B^n$ на $A - B$ дѣлится на n. Итакъ, частное S умноженное на $A - B$, т. е.

$$A^n - B^n \equiv O \ (Mod\ n^{s+1})$$

Слѣдовательно при $t = 1$ теорема доказана. Покажемъ теперь, что сравненіе (56) справедливо при $t = m + 1$, если оно справедливо при $t = m$. Этимъ мы докажемъ его справедливость для всѣхъ $t > O$. Пусть имѣемъ сравненіе:

$$A^{n^m} - B^{n^m} \equiv O \ (Mod\ n^{s+m}) \qquad (57)$$

Перенося $-B^{n^m}$ изъ лѣвой части сравненія (57) въ правую и возводя обѣ части полученнаго сравненія въ степень n, найдемъ:

$$\left(A^{n^m}\right)^n \equiv \left(B^{n^m}\right)^n \ (Mod\ n^{s+m})$$

откуда

$$\left(A^{n^m}\right)^n - \left(B^{n^m}\right)^n \equiv O \ (Mod\ n^{s+m}) \qquad (58)$$

Примѣняя къ сравненію (58) теорему V, найдемъ, что частное отъ дѣленія на

$$A^{n^m} - B^{n^m} \text{ числа } \left(A^{n^m}\right)^n - \left(B^{n^m}\right)^n \qquad (59)$$

дѣлится на n. Слѣдовательно дѣлитель выраженія (59) дѣлится на n^{s+m}, что видно изъ сравненія (57) и частное дѣлится на n, а потому дѣли-

мое (59) раздѣлится на n^{s+m} $n = n^{s+m+1}$. Соображаясь съ этимъ напишемъ: $$\left(A^{n^m}\right)^n - \left(B^{n^m}\right)^n \equiv O\ (Mod\ n^{s+m+1})$$ или $$A^{n^m+1} - B^{n^m+1} \equiv O\ (Mod\ n^{s+m+1})$$

Что и требовалось доказать.

Примѣчаніе. Такъ же легко показать, что при существованіи сравненія $A + B \equiv O\ (Mod\ n^s)$ всегда возможно сравненіе $A^{n^t} + B^{n^t} \equiv O\ (Mod\ n^{s+t})$, если n — число простое и нечетное. Это предложеніе я не доказываю, такъ какъ оно не имѣетъ отношенія къ теоремѣ Фермата. Его легко вывести изъ теоремы IX замѣною B на $-B$ при n нечетномъ. Тою же замѣною легко доказать теоремы IV, VI и VIII на основаніи теоремъ III, V и VII. Я не дѣлаю это потому, что условія относительно n различны и ради большей наглядности.

Теорема X. Если существуетъ сравненіе: $$F^{n(n-1)} \equiv H^n\ (Mod\ n^p + 1) \tag{60}$$ то $$F^{n(n-1)} \equiv 1\ (Mod\ n^p + 1) \text{ и } H^n \equiv 1\ (Mod\ n^p + 1)$$ гдѣ F и H — числа взаимно простыя, а потому порознь на n не дѣлятся, и n — число простое.

Доказательство. Согласно извѣстной теоремѣ Фермата имѣемъ $$F^{n-1} - 1 \equiv O\ (Mod\ n) \tag{61}$$

Примѣняя къ сравненію (61) теорему IX, получимъ: $$(F^{n-1})^{n^p} - 1^{n^p} \equiv O\ (Mod\ n^p + 1)$$ или $$F^{n^p(n-1)} \equiv 1\ (Mod\ n^p + 1) \tag{62}$$

Возводимъ обѣ части сравненія (60) въ степень $n^p - 1$: $$F^{n^p(n-1)} \equiv H^{n^p}\ (Mod\ n^p + 1) \tag{63}$$

Изъ сравненій (62) и (63) найдемъ: $$H^{n^p} \equiv 1\ (Mod\ n^p + 1) \tag{64}$$

Сравненія (62) и (64) возводимъ въ степень n^k, гдѣ k — число произвольное. Эту операцію мы сдѣлаемъ для того, чтобы пока не разбираться въ различныхъ значеніяхъ, которыя можетъ имѣть p. Получимъ: $$F^{n^p+k(n-1)} \equiv 1\ (Mod\ n^p + 1) \tag{65}$$ $$H^{n^p+k} \equiv 1\ (Mod\ n^p + 1) \tag{66}$$

Покажемъ теперь, что показатель $p + k$ постепенными пониженіями на 2 единицы всегда можетъ быть сведенъ къ единицѣ. Помноживъ сравненіе (60) на F^n, найдемъ: $$F^{n^2} \equiv (FH)^n\ (Mod\ n^p + 1) \tag{67}$$

Возведемъ сравненіе (67) въ степень $n^{p+k-2}(n-1)$: $$F^{n^p+k(n-1)} \equiv (FH)^{n^p+k-1(n-1)}\ (Mod\ n^p + 1) \tag{68}$$

Изъ сравненій (65) и (68) имѣемъ :

$$(FH)^{n^p+k-1(n-1)} \equiv 1 \ (Mod\ n^{p+1}) \tag{69}$$

Помноживъ сравненіе (67) на H^{n^2}, найдемъ :

$$(FH)^{n^2} \equiv F^n\ H^{n^3} \ (Mod\ n^{p+1}) \tag{70}$$

Возводимъ сравненіе (70) въ степень $n^p+k-3\,(n-1)$:

$$(FH)^{n^p+k-1(n-1)} \equiv F^{n^p+k-2(n-1)}\ H^{n^p+k(n-1)}\ (Mod\ n^{p+1}) \tag{71}$$

Изъ сравненій (69) и (71) имѣемъ :

$$F^{n^p+k-2(n-1)}\ H^{n^p+k(n-1)} \equiv 1 \ (Mod\ n^{p+1}) \tag{72}$$

Возведя сравненіе (66) въ степень $n-1$, получимъ :

$$H^{n^p+k(n-1)} \equiv 1 \ (Mod\ n^{p+1}) \tag{73}$$

Изъ сравненій (72) и (73) найдемъ :

$$F^{n^p+k-2(n-1)}\ H^{n^p+k(n-1)} \equiv H^{n^p+k(n-1)} \ (Mod\ n^{p+1}) \tag{74}$$

Сокративъ обѣ части сравненія (74) на общаго множителя, получимъ :

$$F^{n^p+k-2(n-1)} \equiv 1 \ (Mod\ n^{p+1}) \tag{75}$$

Возводимъ сравненіе (60) въ степень n^p+k-3 :

$$F^{n^p+k-2(n-1)} \equiv H^{n^p+k-2} (Mod\ n^{p+1}) \tag{76}$$

Изъ сравненій (75) и (76) найдемъ :

$$H^{n^p+k-2} \equiv 1 \ (Mod\ n^{p+1}) \tag{77}$$

Такимъ образомъ мы нашли способъ понизить показатель $p+k$ на двѣ единицы, что видно изъ сопоставленія сравненій (65) и (66) съ (75) и (77). Повторяя тотъ же пріемъ, мы можемъ снова понизить показатель на 2 единицы и т. д. Докажемъ для большей убѣдительности, что, понизивъ показатель $p+k$ на $2m$ единицъ, мы можемъ понизить его на $2m+2$, если $p+k-2m > 2$.

Итакъ допустимъ, что мы пришли къ сравненіямъ

$$F^{n^p+k-2m(n-1)} \equiv 1 \ (Mod\ n^{p+1}) \tag{78}$$

$$H^{n^p+k-2m} \equiv 1 \ (Mod\ n^{p+1}) \tag{79}$$

Возводимъ сравненіе (67) въ степень $n^p+k-2m-2\,(n-1)$

$$F^{n^p+k-2m(n-1)} \equiv (FH)^{n^p+k-2m-1(n-1)} \ (Mod\ n^{p+1}) \tag{80}$$

Изъ сравненій (78) и (80) имѣемъ :

$$(FH)^{n^p+k-2m-1(n-1)} \equiv 1 \ (Mod\ n^{p+1}) \tag{81}$$

Возводимъ сравненіе (70) въ степень $n^p+k-2m-3\,(n-1)$

$$(FH)^{n^p+k-2m-1(n-1)} \equiv$$

$$\equiv F^{n^p+k-2m-2(n-1)}\ H^{n^p+k-2m(n-1)}\ (Mod\ n^{p+1}) \tag{82}$$

Изъ сравненій (81) и (82) имѣемъ:

$$F^{np+k-2m-2(n-1)} H^{np+k-2m(n-1)} \equiv 1 \ (Mod\ n^{p+1}) \quad (83)$$

Возводимъ сравненіе (79) въ степень $n-1$

$$H^{np+k-2m(n-1)} \equiv 1 \ (Mod\ n^{p+1}) \quad (84)$$

Изъ сравненій (83) и (84) находимъ:

$$F^{np+k-2m-2(n-1)} H^{np+k-2m(n-1)} \equiv$$

$$\equiv H^{np+k-2m(n-1)} \ (Mod\ n^{p+1})$$

Сокративъ послѣднее сравненіе, получимъ:

$$F^{np+k-2m-2(n-1)} \equiv 1 \ (Mod\ n^{p+1}) \quad (85)$$

Сравненіе (60) возведемъ въ степень $n^{p+k-2m-3}$

$$F^{np+k-2m-2(n-1)} \equiv H^{np+k-2m-2} \ (Mod\ n^{p+1}) \quad (86)$$

Изъ сравненій (85) и (86) находимъ

$$H^{np+k-2m-2} \equiv 1 \ (Mod\ n^{p+1}) \quad (87)$$

Сравненія (85) и (87) показываютъ, что постепенными пониженіями на 2 единицы мы всегда можемъ показатель $p+k$ уменьшить на какое угодно четное и положительное число такъ, чтобы разность была числомъ положительнымъ. Разберемъ теперь два возможныхъ случая:

1) p — число четное. Такъ какъ k — число произвольное, то въ данномъ случаѣ мы должны его взять нечетнымъ: тогда $p+k$ будетъ числомъ нечетнымъ, а $p+k-1$ — числомъ четнымъ. Повторяя нашъ пріемъ $\frac{p+k-1}{2}$ разъ, мы сведемъ показатель степени при n въ сравненіяхъ (65) и (66) къ единицѣ.

2) p — число нечетное. Въ этомъ случаѣ k должно быть четнымъ, а потому $p+k$ — число нечетное, а $p+k-1$ — число четное. И въ этомъ случаѣ, повторяя указанный пріемъ $\frac{p+k-1}{2}$ разъ, приведемъ показатель степени при n въ сравненіяхъ (65) и (66) къ единицѣ. Итакъ, въ обоихъ случаяхъ мы получимъ сравненія

$$F^{n(n-1)} \equiv 1 \ (Mod\ n^{p+1})$$

$$H^{n} \equiv 1 \ (Mod\ n^{p+1})$$

Что и требовалось доказать.

Примѣчаніе. Удобство введенія k въ доказательство заключается еще въ томъ, что намъ нѣтъ надобности разбирать отдѣльно случаи, когда $p=1$ или $p=2$.

Сравненіе (62), которое мы нашли помощью теоремы IX, непосредственно слѣдуетъ изъ теоремы Эйлера:

$$A^{\varphi(N)} \equiv 1 \ (Mod\ N)$$

Какъ я уже сказалъ, я умышленно не пользуюсь этой теоремой.

Теорема XI. Если $n > 2$ и $p \geqq 1$ и существуютъ сравненія:

$$M \equiv O\ (Mod\ n^p) \tag{88}$$

$$N \equiv O\ (Mod\ n^{np-1}) \tag{89}$$

то высшая степень, въ которой n входитъ дѣлителемъ въ число $M \pm N$, есть p, когда M не можетъ дѣлиться на $n^p + 1$

Доказательство. Допустимъ противное. Пусть высшая степень, въ которой n входитъ въ число $M \pm N$, будетъ q больше или меньше p. При q большемъ p можемъ написать:

$$M \pm N \equiv O\ (Mod\ n^p + 1) \tag{90}$$

При нашихъ условіяхъ относительно n и p

$$np - 1 \geqq p + 1 \tag{91}$$

Такъ какъ, допустивъ противное, получимъ $np - 1 < p + 1$, или $p\,(n-1) < 2$, а тѣмъ болѣе $n - 1 < 2$, или $n < 3$, что возможно только тогда, когда $n \leqq 2$, а это противорѣчитъ условію. Изъ сравненія (89) и неравенства (91) имѣемъ:

$$N \equiv O\ (Mod\ n^p + 1) \tag{92}$$

Изъ сравненій (90) и (92) имѣемъ:

$$M \equiv O\ (Mod\ n^p + 1)$$

Что противорѣчитъ условію. Слѣдовательно q не можетъ быть больше p. Допустимъ, что $q < p$. Это очевидно невозможно. Изъ сравненія (92) вытекаетъ, что

$$N \equiv O\ (Mod\ n^p) \tag{93}$$

Изъ сравненій (88) и (93) имѣемъ:

$$M \pm N \equiv O\ (Mod\ n^p)$$

Это сравненіе доказываетъ, что q не можетъ быть меньше p. Остается единственно возможный случай $q = p$, и теорема доказана.

Часть II.

Глава I. Основныя свойства уравненія $x^n + y^n = z^n$

Теорема XII. Если равенство

$$x^n + y^n = z^n \tag{94}$$

не можетъ существовать для какого-либо показателя n, когда x, y и z числа цѣлыя и взаимно простыя, то это равенство невозможно и въ томъ случаѣ, когда x, y и z будутъ числами цѣлыми, имѣющими общихъ дѣлителей.

Доказательство. Допустимъ противное, т. е. предположимъ, что равенство (94) возможно при нашихъ условіяхъ, когда x, y и z числа цѣлыя, имѣющія общихъ дѣлителей. Во первыхъ, очевидно, что въ

томъ случаѣ, когда два числа изъ трехъ данныхъ имѣютъ общій множитель, а третье число на этотъ множитель не дѣлится, то равенство (94) существовать не можетъ. Во вторыхъ, когда x, y и z общимъ наибольшимъ дѣлителемъ имѣютъ r, то x^n, y^n и z^n каждое раздѣлится на r^n, а потому, сокращая равенство (94) на r^n, получимъ равенство того же вида, но съ числами взаимно простыми, а такое равенство по условію существовать не можетъ. Слѣдовательно, наше допущеніе невозможно, и теорема доказана.

Слѣдствіе. Эта теорема даетъ право доказать «великое предложеніе» при томъ условіи, что x, y и z числа взаимно простыя. Поэтому въ дальнѣйшемъ изложеніи я всегда буду предполагать, что x, y и z числа взаимно простыя, когда дѣлаю допущеніе, что равенству (94) можно удовлетворить цѣлыми числами.

Теорема XIII. Если уравненію (94) нельзя удовлетворить цѣлыми числами, когда n — число простое и большее двухъ и когда $n = 4$, то это уравненіе нельзя рѣшить въ цѣлыхъ числахъ при всякомъ n большемъ двухъ.

Доказательство. Такъ какъ показатель степени большій двухъ можетъ быть или нечетнымъ простымъ числомъ, или какимъ либо составнымъ, содержащимъ множителемъ одно изъ нечетныхъ простыхъ чиселъ, или, наконецъ, имѣть форму 2^m, то намъ достаточно показать, что при невозможности существованія равенства (94) при какомъ-либо n и x, y и z числахъ цѣлыхъ, не можетъ существовать равенство:

$$x^{nt} + y^{nt} = z^{nt} \tag{95}$$

Это очевидно изъ слѣдующаго. Равенство (95) можно написать такъ:

$$(x^t)^n + (y^t)^n = (z^t)^n$$

гдѣ x^t, y^t и z^t — числа цѣлыя, а такое равенство по условію существовать не можетъ. Этимъ и доказывается предложенная теорема.

Слѣдствіе. Какъ слѣдствіе изъ теоремы XIII вытекаетъ то, что «великое предложеніе» достаточно доказать при n числѣ простомъ нечетномъ и большемъ двухъ и при $n = 4$.

Глава II. Показатель n — число простое.

Теорема XIV. Уравненіе (94) разрѣшимо въ цѣлыхъ числахъ при $n = 1$ и при $n = 2$.

Доказательство. Очевидно, что при $n = 1$ уравненіе (94) разрѣшимо въ цѣлыхъ числахъ, такъ какъ стоитъ взять любыя два числа и найти ихъ сумму, чтобы получить частныя значенія для x, y и z. При $n = 2$, полагая, что

$$x = 2AB\,;\; y = A^2 - B^2\,;\; z = A^2 + B^2,$$

гдѣ A и B произвольныя цѣлыя числа, и подставляя значенія x, y и z въ уравненіе (94), имѣемъ:

$$(2AB)^2 + (A^2 - B^2)^2 = (A^2 + B^2)^2$$

простое тождество.

Теорема XV. Если уравненіе

$$x^n + y^n = z^n \tag{96}$$

можно рѣшить въ цѣлыхъ числахъ при n числѣ простомъ, то

$$x + y - z \equiv O \ (Mod\ n)$$

Доказательство. Каковы бы ни были числа x, y и z, какъ слѣдствіе теоремы Фермата, всегда возможны сравненія :

$$x^n \equiv x \ (Mod\ n) \tag{97}$$

$$y^n \equiv y \ (Mod\ n) \tag{98}$$

$$z^n \equiv z \ (Mod\ n) \tag{99}$$

Складывая сравненія (97) съ (98) и затѣмъ вычитая (99), получимъ :

$$x^n + y^n - z^n \equiv x + y - z \ (Mod\ n) \tag{100}$$

Изъ сравненія (100) и равенства (96) найдемъ :

$$x + y - z \equiv O \ (Mod\ n)$$

Что и требовалось доказать.

Слѣдствіе. Согласно доказанной теоремѣ при существованіи равенства (96), когда n — число простое, $x + y - z$ всегда дѣлится на n, а потому при $n > 1$ мы можемъ написать равенство :

$$x + y - z = n^{\omega} M \tag{101}$$

гдѣ M на n не дѣлится, а ω — высшая степень, въ которой n входитъ дѣлителемъ въ число $x + y - z$, больше нуля. Въ дальнѣйшемъ мы ω всегда будемъ давать указанное значеніе.

Теорема XVI. Если можетъ существовать равенство :

$$x^n + y^n = z^n \tag{102}$$

гдѣ n — число простое, а x, y и z — числа цѣлыя, то

$$(z - x)^n + (z - y)^n - (x + y)^n \equiv O \ (Mod\ n^{\omega + 1})$$

Доказательство. Согласно нашимъ условіямъ, равенство (101) даетъ право написать сравненіе :

$$x + y - z \equiv O \ (Mod\ n^{\omega}) \tag{103}$$

Сравненіе (103) напишемъ въ такихъ видахъ :

$$x \equiv z - y \ (Mod\ n^{\omega}) \tag{104}$$

$$y \equiv z - x \ (Mod\ n^{\omega}) \tag{105}$$

$$x + y \equiv z \ (Mod\ n^{\omega}) \tag{106}$$

Примѣняя къ сравненіямъ (104), (105) и (106) теорему IX, получимъ :

$$x^n \equiv (z - y)^n \ (Mod\ n^{\omega + 1}) \tag{107}$$

$$y^n \equiv (z - x)^n \ (Mod\ n^{\omega + 1}) \tag{108}$$

$$(x + y)^n \equiv z^n \ (Mod\ n^{\omega + 1}) \tag{109}$$

Складывая сравненія (107), (108) и (109) найдемъ :

$$x^n + y^n + (x + y)^n \equiv (z - y)^n + (z - x)^n + z^n \ (Mod\ n^{\omega + 1}) \tag{110}$$

Изъ сравненія (110) и равенства (102) найдемъ сравненіе :

$$(x + y)^n \equiv (z - y)^n + (z - x)^n \ (Mod\ n^{\omega + 1})$$

которое можно написать такъ :

$$(z-x)^n+(z-y)^n-(x+y)^n \equiv O\ (Mod\ n^{\omega+1})$$

Что и требовалось доказать.

Теорема XVII. Если можетъ существовать равенство :

$$x^n+y^n=z^n \tag{111}$$

при $n>2$ числѣ простомъ, а потому нечетномъ, и при x, y и z числахъ цѣлыхъ ; то :

$$(z-y)^n \equiv z-y\ (Mod\ n^{\omega+1}) \tag{112}$$

$$(z-x)^n \equiv z-x\ (Mod\ n^{\omega+1}) \tag{113}$$

$$(x+y)^n \equiv x+y\ (Mod\ n^{\omega+1}) \tag{114}$$

Доказательство. Чтобы доказать правдивость сравненія (112), разберемъ два случая, которые только и могутъ встрѣтиться :

1) $z-y$ дѣлится на n. Написавъ равенство (111) въ формѣ :

$$x^n=z^n-y^n \tag{115}$$

видимъ, что правая часть равенства (115) дѣлится на $z-y$, а потому дѣлится и на n. Слѣдовательно и x^n дѣлится на n ; откуда должны заключить, что x дѣлится на n, такъ какъ n — число простое по условію. Пусть въ такомъ случаѣ высшая степень, въ которой n входитъ дѣлителемъ въ число x, есть p, а потому можемъ написать :

$$x \equiv O\ (Mod\ n^p) \tag{116}$$

$$x^n \equiv O\ (Mod\ n^{np}) \tag{117}$$

Изъ равенства (115) и сравненія (117) найдемъ :

$$z^n-y^n \equiv O\ (Mod\ n^{np}) \tag{118}$$

Примѣняя къ сравненію (118) теорему VII, найдемъ :

$$z-y \equiv O\ (Mod\ n^{np-1}) \tag{119}$$

Возведемъ сравненіе (119) въ степень n:

$$(z-y)^n \equiv O\ (Mod\ n^{np-1}) \tag{120}$$

Такъ какъ при $n>2$ и $p \geqq 1$,

$$np-1 \geqq p+1, \tag{121}$$

что мы подтвердили при доказательствѣ теоремы XI, то изъ сравненій (119) и (120) и неравенства (121) имѣемъ :

$$z-y \equiv O\ (Mod\ n^{p+1})$$

$$(z-y)^n \equiv O\ (Mod\ n^{p+1})$$

Откуда заключаемъ, что

$$(z-y)^n \equiv z-y\ (Mod\ n^{p+1}) \tag{122}$$

Согласно нашему условію относительно p и теоремѣ XI изъ сравненій (116) и (119) найдемъ, что p есть высшая степень, въ которой n входитъ дѣлителемъ въ число : $x+y-z$, а потому $p=\omega$. Соображаясь съ этимъ сравненіе (122) напишемъ :

$$(z-y)^n \equiv z-y\ (Mod\ n^{\omega+1})$$

2) Если $z-y$ не дѣлится на n, то и z^n-y^n на n не дѣлится, такъ какъ въ противномъ случаѣ по теоремѣ I и $z-y$ дѣлилось бы на n. При такихъ условіяхъ согласно теоремѣ III найдемъ, что $z-y$ и частное C отъ дѣленія z^n-y^n на $z-y$ не могутъ имѣть общихъ дѣлителей большихъ единицы; но x^n содержитъ всѣ простые дѣлители въ степеняхъ кратныхъ n, а потому это относится и къ z^n-y^n, какъ къ равному x^n. Соображаясь съ этимъ, найдемъ:

$$z-y=a^n \tag{123}$$

$$C=b^n \tag{124}$$

гдѣ a и b — числа взаимно простыя. Перемноживъ равенства (123) и (124), найдемъ:

$$(z-y)\,C=a^n\,b^n=z^n-y^n=x^n \tag{125}$$

При нашихъ условіяхъ $x+y-z\equiv O\ (Mod\ n^\omega)$; откуда:

$$x\equiv z-y\ (Mod\ n^\omega) \tag{126}$$

Примѣняя къ сравненію (126) теорему IX, найдемъ:

$$x^n\equiv(z-y)^n\ (Mod\ n^\omega+1) \tag{127}$$

Подставивъ въ сравненіе (127) значенія x^n и $z-y$ изъ равенствъ (125) и (123), найдемъ:

$$a^n\,b^n\equiv a^{n^2}\ (Mod\ n^\omega+1)$$

или

$$a^{n(n-1)}\equiv b^n\ (Mod\ n^\omega+1) \tag{128}$$

такъ какъ a^n, какъ равное $z-y$, на n не дѣлится.

Изъ сравненія (128) по теоремѣ X имѣемъ:

$$a^{n(n-1)}\equiv 1\ (Mod\ n^\omega+1) \tag{129}$$

Помноживъ сравненіе (129) на a^n, найдемъ:

$$(a^n)^n\equiv a^n\ (Mod\ n^\omega+1) \tag{130}$$

Замѣняя въ сравненіи (130) a^n его значеніемъ изъ равенства (123), имѣемъ:

$$(z-y)^n\equiv z-y\ (Mod\ n^\omega+1)$$

Такимъ образомъ находимъ, что сравненіе (112) справедливо.

Для доказательства того, что сравненіе (113) при нашихъ условіяхъ имѣетъ мѣсто, замѣчаемъ, что x и y входятъ симметрично въ равенство (111), а потому все сказанное относительно $z-y$ будетъ примѣнимо и къ $z-x$.

Для доказательства справедливости сравненія (114) снова разсмотримъ два возможныхъ случая:

1) $x+y$ дѣлится на n. Изъ равенства (111) видно, что при n нечетномъ лѣвая его часть дѣлится на $x+y$, а потому дѣлится и на n. Слѣдовательно и z^n дѣлится на n, какъ равное x^n+y^n. Изъ этого заключаемъ, что z дѣлится на n, такъ какъ n — число простое по условію. Допустимъ въ такомъ случаѣ, что S будетъ высшею степенью, въ которой n входитъ множителемъ въ число z. Тогда имѣемъ:

$$z\equiv o\ (Mod\ n^S) \tag{131}$$

$$z^n \equiv o\ (Mod\ n^{ns}) \tag{132}$$

Изъ сравненія (132) и равенства (111) находимъ:

$$x^n + y^n \equiv o\ (Mod\ n^{ns}) \tag{133}$$

Примѣняя къ сравненію (133) теорему VIII, получимъ:

$$x + y \equiv o\ (Mod\ n^{ns-1}) \tag{134}$$

Возведемъ сравненіе (134) въ степень n:

$$(x + y)^n \equiv o\ (Mod\ n^{ns-1}) \tag{135}$$

Изъ сравненій (134) и (135) имѣемъ:

$$(x + y)^n \equiv x + y\ (Mod\ n^{ns-1}) \tag{136}$$

При $n > 2$ и $s \geqq 1$, какъ это мы уже знаемъ,

$$ns - 1 \geqq s + 1 \tag{137}$$

Соображаясь съ (136) и (137), напишемъ

$$(x + y)^n \equiv x + y\ (Mod\ n^{s+1}) \tag{138}$$

Изъ нашего условія относительно s и сравненій (131) и (134) находимъ, что s есть высшая степень, въ которой n входитъ дѣлителемъ въ число $x + y - z$, согласно теоремѣ XI; а потому $s = \omega$. Слѣдовательно, сравненіе (138) принимаетъ видъ:

$$(x + y)^n \equiv x + y\ (Mod\ n^{\omega+1})$$

2) Если $x + y$ не дѣлится на n, то и $x^n + y^n$ на n не дѣлится, такъ какъ въ противномъ случаѣ по теоремѣ II и $x + y$ дѣлилось бы на n. При такихъ условіяхъ, согласно теоремѣ IV, $x + y$ и частное V отъ дѣленія $x^n + y^n$ на $x + y$ не могутъ имѣть общихъ дѣлителей большихъ единицы; но z^n содержитъ всѣ простые дѣлители въ степеняхъ кратныхъ n, а потому это относится и къ $x^n + y^n$, какъ къ равному z^n. Соображаясь съ этимъ, найдемъ:

$$x + y = c^n \tag{139}$$

$$V = d^n \tag{140}$$

Изъ равенствъ (139) и (140) находимъ:

$$(x + y)\ V = c^n\ d^n = x^n + y^n = z^n \tag{141}$$

Здѣсь c и d — числа взаимно простыя.

При нашихъ условіяхъ $x + y - z \equiv o\ (Mod\ n^{\omega})$; откуда

$$x + y \equiv z\ (Mod\ n^{\omega}) \tag{142}$$

Примѣняя къ сравненію (142) теорему IX, получимъ:

$$(x + y)^n \equiv z^n\ (Mod\ n^{\omega+1}) \tag{143}$$

Подставивъ въ сравненіе (143) значенія $x + y$ и z^n изъ равенствъ (139) и (141), получимъ:

$$c^{n^2} \equiv c^n\ d^n\ (Mod\ n^{\omega+1})$$

откуда:

$$c^{n(n-1)} \equiv d^n\ (Mod\ n^{\omega+1}) \tag{144}$$

такъ какъ c^n, какъ равное $x + y$, не дѣлится на n. Изъ сравненія (144), согласно теоремѣ X, найдемъ:

$$c^{n(n-1)} \equiv 1\ (Mod\ n^{\omega+1}) \tag{145}$$

Помножимъ сравненіе (145) на c^n; имѣемъ:

$$(c^n)^n \equiv c^n \ (Mod\ n^{\omega+1}) \qquad (146)$$

Подставивъ вмѣсто c^n его значеніе изъ равенства (139), найдемъ:

$$(x+y)^n \equiv x+y \ (Mod\ n^{\omega+1})$$

Изъ всего сказаннаго приходимъ къ заключенію, что наша теорема вѣрна.

Теорема XVIII. Уравненію:

$$x^n + y^n = z^n \qquad (147)$$

нельзя удовлетворить цѣлыми числами, если n — число простое, больше двухъ и потому нечетное.

Доказательство. Допустимъ, что x, y и z — числа цѣлыя. Въ такомъ случаѣ, согласно теоремѣ XV, $x+y-z$ дѣлится на n, и по теоремѣ XVII имѣемъ:

$$(z-x)^n \equiv z-x \ (Mod\ n^{\omega+1}) \qquad (148)$$

$$(z-y)^n \equiv z-y \ (Mod\ n^{\omega+1}) \qquad (149)$$

$$(x+y)^n \equiv x+y \ (Mod\ n^{\omega+1}) \qquad (150)$$

гдѣ ω, какъ мы условились выше, есть высшая степень, въ которой n входитъ дѣлителемъ въ число $x+y-z$. Складывая сравненія (148) и (149) и затѣмъ вычитая сравненіе (150), найдемъ:

$$(z-x)^n + (z-y)^n - (x+y)^n \equiv 2(z-x-y) \ (Mod\ n^{\omega+1}) \qquad (151)$$

При нашихъ условіяхъ, согласно теоремѣ XVI, имѣемъ:

$$(z-x)^n + (z-y)^n - (x+y)^n \equiv o \ (Mod\ n^{\omega+1}) \qquad (152)$$

Изъ сравненій (151) и (152) имѣемъ:

$$2(x+y-z) \equiv o \ (Mod\ n^{\omega+1}) \qquad (153)$$

Сравненіе (153) возможно только при n равномъ двумъ или единицѣ. Въ самомъ дѣлѣ:

$$x+y-z = n^{\omega} M \qquad (154)$$

гдѣ M на n не дѣлится, а потому, подставляя значеніе $x+y-z$ изъ равенства (154) въ сравненіе (153) и сокращая послѣднее на M, найдемъ:

$$2n^{\omega} \equiv o \ (Mod\ n^{\omega+1}) \qquad (155)$$

Сокративъ въ сравненіи (155) число и модуль на n^{ω}, получимъ:

$$2 \equiv o \ (Mod\ n)$$

что при нашихъ условіяхъ невозможно, а потому наше допущеніе не имѣетъ мѣста и теорема доказана.

Глава III $n=4$. Заключеніе.

При $n=4$ теорему Фермата, какъ я уже сказалъ, доказалъ Эйлеръ. Желающіе познакомиться съ этимъ доказательствомъ могутъ найти его во многихъ сочиненіяхъ по теоріи чиселъ и сравненій. Замѣчу между прочимъ, что на русскомъ языкѣ оно имѣется въ курсѣ «Высшей Алгебры», сочиненіе профессора М. Е. Ващенко-Захар-

ченко, изданіе 1887 г. стр. 185 и 186. Я не привожу его ради сокращенія мѣста и потому еще, что оно извѣстно всѣмъ, занимающимся теоріей чиселъ.

Заключеніе.

Изъ всего сказаннаго вытекаетъ, что „. . . . невозможно разложить полный кубъ на сумму двухъ кубовъ, четвертую степень на сумму двухъ четвертыхъ степеней, вообще, какую-либо степень на сумму двухъ степеней съ тѣмъ же показателемъ, если послѣдній больше двухъ“, такъ какъ нельзя удовлетворить цѣлыми числами уравненію: $x^n + y^n = z^n$ *при* $n > 2$.

Примѣчаніе. Любопытнѣе всего то, что, доказавъ «великое предложеніе», очень просто можно доказать интересную теорему: Уравненію $x^n + y^n = z^n$ нельзя удовлетворить не только цѣлыми, но вообще числами соизмѣримыми съ единицей при n — числѣ цѣломъ, положительномъ или отрицательномъ, по абсолютной величинѣ большемъ двухъ. Другими словами, уравненіе $x^n + y^n = z^n$ при $n > 2$ или $n < -2$, числѣ цѣломъ, можетъ имѣть только мнимые корни и дѣйствительные, изъ которыхъ по крайней мѣрѣ одинъ будетъ числомъ несоизмѣримымъ.

Доказательство. Мы показали, что при $n > 2$, числѣ цѣломъ, уравненію $x^n + y^n = z^n$ нельзя удовлетворить цѣлими числами. Допустимъ, что оно имѣетъ дробные корни, т. е. $\left(\frac{a}{b}\right)^n + \left(\frac{c}{d}\right)^n = \left(\frac{e}{f}\right)^n$, гдѣ a, b, c, d, e и f — числа цѣлыя. Тогда имѣемъ: $(adf)^n + (bcf)^n = (bde)^n$, а такое равенство невозможно. Значитъ наше допущеніе не имѣетъ мѣста. Теперь покажемъ, что уравненіе $x^{-n} + y^{-n} = z^{-n}$ не имѣетъ соизмѣримыхъ корней. Его можно написать въ такомъ видѣ: $\frac{1}{x^n} + \frac{1}{y^n} = \frac{1}{z^n}$ и еще $(yz)^n + (xz)^n = (xy)^n$, а такое равенство, какъ мы только что доказали, при x, y и z числахъ соизмѣримыхъ существовать не можетъ. Этимъ и доказывается теорема.

Сентябрь 1909 г. — Сентябрь 1910 г.

Петръ Москальскій.

Цѣна 50 коп.