Теорія чиселъ.

Лекціи проф. Ландау, читанныя в Гёттингенскомъ университетѣ в теченіе лѣтняго семестра 1911 г.

Настоящій курсъ состоитъ изъ 3х отдѣловъ:

1) Ученіе о дѣлимости.
2) Числовыя уравненія.
3) Разложеніе цѣлыхъ чиселъ на суммы одинаковыхъ степеней.

Отдѣлъ I. Ученіе о дѣлимости.

Имѣемъ a и b — 2 цѣлыхъ положительныхъ числа. Мы утверждаемъ, что всегда можно разрѣшить в цѣлыхъ положит. числахъ уравненіе

$$a = bq + r$$

(или найти 2 цѣлыхъ пол. числа q и r, удовлетворяющія написанному равенству), причемъ

$$q \geqq 0. \quad 0 \leqq r < b.$$

Доказательство: пишемъ рядъ чиселъ:

$$a,\ a-b,\ a-2b, \ldots$$

~~В этомъ рядѣ~~ Продолжая этотъ рядъ, мы всегда дойдемъ до отрицательных чисел; в самом деле, число $a - ab$ равно 0 или меньше $a - ab = a(1-b) \leqq 0$. Вычитая еще раз a, получим наверно отриц. число. Итак, мы найдем всегда число q такое, что $a - qb \geqq 0$, между тем как $a - (q+1)b < 0$. Назвав разность в левой части r, мы видим, что в 1м случае $r \geqq 0$, а $r - b < 0$, т.е. $r < b$. Остается доказать, что (при условии $a > 0$) $q \not< 0$. Если бы было $q < 0$, то $qb \leqq -b$, $qb + r < 0$, т.е. $a < 0$, что противоречит условию. Итак, q не отрицательно.

Докажем, что найденное решение единственное. Допустим, что существуют 2 решения:

$$a = bq + r, \quad a = bq_1 + r_1 \quad (0 \leqq r_1 < b)$$

~~Из чисел~~ $q \neq q_1$; предположим $q > q_1$. Вычитаем:

$$0 = b(q - q_1) + r - r_1 \quad \text{или} \quad r_1 - r = b(q - q_1)$$

Левая часть $\leqq b - 1$, а правая $\geqq b$; это невозможно, значит найденное решение единственное.

Разделив обе части найденного равенства на b, имеем

$$\frac{a}{b} = q + \frac{r}{b}, \text{ где } \frac{r}{b} \text{ правильная дробь.}$$

q есть наибольшее положит. число, заключающееся в дроби $\frac{a}{b}$.

Пусть вообще $N > 0$ — любое положит. число (хоть бы дробь)

Наибольшее полож. целое число, заключающееся в x, будем обозначать символом $E(x)$ или $[x]$. В нашем случае имеем: $q = [\frac{a}{b}]$.

$[x]$ удовлетворяет неравенству: ~~$x \geq [x] > x-1$~~. $[x] \leq x < [x]+1$.

Взявши b равным, напр. 6, мы все числа разбили на 6 классов, ~~в которых r~~ с соответственно значениями $r = 0, 1, 2, 3, 4, 5$.

Из этих классов ~~тот~~, где $r=0$, имеет особое значение; ~~в нем~~ 6 является делителем каждого числа этого класса.

Будем обозначать то, что a делится на b, символом $b|a$.

Теорема 1. Условие: $b|a$, $c|b$. Утверждение $c|a$.

Доказ. $b|a$ значит $a=qb$, $c|b$ зн. $b=q'c$; $a=qq'c$, т.е. $c|a$.

Теорема 2. Усл. $b|a$, $b|a_1$; тр. док. $b|a+a_1$, $b|a-a_1$.

Док. $a=qb$, $a_1=q_1b$; $a+a_1=(q+q_1)b$; $a-a_1=(q-q_1)b$, т.е. $b|a\pm a_1$

Теорема 3. Дано: $b|a$, $b|a_1$; x, y — любые ц. полож. числа. Тр. док.: $b|ax+a_1y$; Доказ. $b|a|ax$; $b|a_1|a_1y$; сл. $b|ax+a_1y$.

Глава 2. О простых числах.

Каждое число имеет по кр. мере одного делителя — самого себя: $a|a$; отсюда $a = a.1$, т.е. все числа, начиная с 2, имеют еще 2-ой делитель, 1. Числа, не имеющие иных делителей, кроме самого себя и 1, наз. ~~первоначальными~~ простыми

Т. обр. по отношенію к дѣлимости всѣ числа дѣлятся на 3 класса: 1) единица, 2) простыя числа, 3) составныя числа.

<u>Теорема.</u> Каждое число м. б. разложено на разложить(ся) произведеніе произв. простых чисел и притом единственным образом.

I. 1) a, большее 1, имѣет по крайней мѣрѣ одного простого дѣлителя p. Док.: если a простое число, утвержденіе вѣрно, если a не простое, оно м. быть представлено в видѣ произведенія 2х множителей, из коих наименьшій $m>1$. Если m простое число, положеніе доказано, если нѣт, представляем его также в видѣ $n.n_1$, пусть $n \geq n_1 > 1$ и т. д. $n<m$. Этот процесс не мож. продолжаться безконечно, т. к. каждый слѣд. дѣлитель на цѣлое число единиц меньше предшествующаго. Итак, мы непремѣнно найдем простой дѣлитель числа a;

2). Дано: $a>1$; тр. док.: $a=p_1p_2 \ldots p_\lambda$. Доказ. Если a простое, теор. очевидна, если нѣт, то по доказанному $a=p_1a_1$. Если a_1 простое, теор. доказана, если нѣт, то $a_1=p_2a_2$, $a=p_1p_2a_2$ и т. д. Получим ряд чисел $a>a_1>a_2>\ldots$ Процесс не может продолжаться до безконечности, и $a_\lambda=p_\lambda=$ простому числу. Тогда получим искомое разложеніе

3) Дано: $b<p$, $c<p$. Тр. док. $p\nmid bc$. Док-во. Пусть $p|bc$. Рассмотрим ряд чисел:

$$bc,\ b(c-1), \dots\ b.2,\ b.1.$$

Если $c=1$, то теор. очевидна; если $c>1$, то в этом ряду, идя (начиная) с правой стороны, мы встретим первое число, делящееся на p; $p|b\gamma$; $1<\gamma\le c$, т.е. $1<\gamma<p$. Делим p на γ;

$p=q\gamma+r$; $0\le r<\gamma$. Но $r\neq 0$, т.к. p простое число, $r<\gamma$

$br=b(p-q\gamma)=bp-qb\gamma$. По предположению $p|b\gamma$, т.е. $p|br$, и $b\gamma$ уже не 1-ое число, делящееся на p в нашем ряду. Мы пришли к противоречию, значит предположение не верно.

4) Дано: $p\nmid b$, $p\nmid c$; тр. док.: $p\nmid bc$. Доказательство: $b=qp+b_1$, где $0\le b_1<p$ или $1\le b_1<p$. $c=q'p+c_1$, где $1\le c_1<p$. По предыдущему $p\nmid b_1c_1$. $bc=qq'p^2+qc_1p+q'b_1p+b_1c_1=Mp+b_1c_1$; $bc-Mp=b_1c_1$; значит $p\nmid bc$

5) Дано: $p\nmid b_1, p\nmid b_2, \dots p\nmid b_k$; тр. док.: $p\nmid b_1b_2\dots b_k$. Доказ.: $p\nmid b_1b_2$ по док., и $p\nmid b_3$, сл. $p\nmid b_1b_2b_3$ и т. д. Наконец найдем $p\nmid b_1b_2\dots b_k$.

II. Докажем, что разложение на простые множители единственное. Пусть имеется 2 разложения:

$$a=p_1p_2\dots p_\lambda\ ;\ a=q_1q_2\dots q_\mu.$$

По теор. 5 q_1 должно делить хоть одно из простых чисел p, напр. p_1

$q_1|p_1$; оба числа простые, $\neq 1$, след. $p_1=q_1$

В предполагаемом равенстве $p_1 p_2 \dots p_\lambda = q_1 q_2 \dots q_\mu$ сокращаем $p_2 p_3 \dots p_\lambda = q_2 q_3 \dots q_\mu$. Таким же способом докажем, что $q_2 = p_2$ и т.д., и число простых множителей $\lambda = \mu$, т.е. оба разложения тождественны.

Докажем, что число простых чисел бесконечно; если бы оно было конечно, то существ. бы последнее простое число p_ν. Составляем выражение

$$2.3.5.7 \dots p_\nu + 1.$$

Это число м. быть простым, тогда теорема доказана, т.к. оно $> p_\nu$. Если же оно составное, то ~~(в его составе) могут~~ оно делится на простое число, кот. наверно больше p_ν; теорема доказана и в этом случае.

Теорема. Если x произвольное целое число, то существует по кр. мере одно простое число p, лежащее в интервале $x < p < x^x$. Доказ. $x! - 1 < x! \leq x^x$. Каждый простой множитель числа $x! - 1$ больше, чем x и меньше (или равен) $x! - 1 < x^x$.

Теорема. Существует бесчисленное множество простых чисел вида $4q+3$. Пусть p_ν последнее число этого вида. Берем число

$$a = 4 p_1 p_2 \dots p_\nu - 1 \quad (p_1, p_2 \dots \text{все первоначальные числа} < p_\nu)$$

Все простые делители числа a больше p_ν и не могут быть все вида $4q+1$, т.к. в этом случае произведение их имело бы вид: $4Q+3$

Заметим, что все простые числа, кроме 2 и 3, могут быть представлены в виде: $6q+1$ или $6q-1$.

Теорема. Существует бесчисленное множество простых чисел вида $6q-1$. Пусть последнее число этого вида есть p_ν; составляем выражение:

$$a = 6(p_1 \cdot p_2 \dots p_\nu) - 1.$$

Все первонач. факторы a больше p_ν, и хоть один из них имеет вид $6q-1$, т. к. иначе было бы $a = 6Q+1$.

Таким же образом выведем, что существует бесчисленное множество простых чисел вида $3q-1$.

Мы убедились, что линейные формы $4x+3$, $3x+2$, $6x+5$ выражают каждая беск. множество простых чисел; эти теоремы являются частными случаями теоремы Dirichlet (1837), состоящей в следующем: линейная форма

$$ax+b,$$

где a и b взаимно простые числа, выражает бесчисленное множество простых чисел.

Пусть g любое целое число; мы всегда можем найти g последовательных чисел $x, x+1, x+2, \dots, x+g-1$, которые все составные; для этого надо положить $x=(g+1)!+2$.

Разложеніе факторіала на простые множители.

Если въ выраженіе $n!$ войдетъ множителемъ въ нѣкоторой степени всякое $p \leqq n$; опредѣлимъ показатель при какомъ-нибудь p. Пусть α есть число чиселъ, кратныхъ p и не превышающихъ n; $\alpha p \leqq n < (\alpha+1)p$, т. е. $\alpha = \left[\frac{n}{p}\right]$. Каждое изъ ~~этихъ~~ чиселъ, кратныхъ p, даетъ въ разложенія $n!$ одного множителя p; всѣ вмѣстѣ они дадутъ въ разложеніи $n!$ множителемъ $p^{\left[\frac{n}{p}\right]}$. Каждое изъ чиселъ, меньшихъ n. и кратныхъ p^2, даетъ въ разложеніи $n!$ сверхъ того множителемъ p; всѣ вмѣстѣ дадутъ $p^{\left[\frac{n}{p^2}\right]}$. Могутъ оказаться числа $< n$ и кратные p^3; они дадутъ въ разложеніи $n!$ $p^{\left[\frac{n}{p^3}\right]}$ и т. д. Такимъ образомъ показатель при p есть $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\dots$, а все разложеніе $n!$ представится въ видѣ

$$n! = \prod_{p \leqq n} p^{\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\dots\left[\frac{n}{p^\alpha}\right]},$$

гдѣ $p^\alpha \leqq n$, а $p^{\alpha+1} > n$, т. е. $\alpha \leqq \frac{\lg n}{\log p}$, $\alpha > \frac{\lg n}{\lg p} - 1$.

О коэффиціентахъ въ разложеніи бинома Ньютона.

Коэф. разложенія бинома Ньютона $(x+y)^m$ для m цѣлаго положит. имѣютъ видъ $\binom{m}{\nu} = \frac{m(m-1)\dots(m-\nu+1)}{\nu!}$. Докажемъ, что это цѣлыя числа.

$\binom{m}{\nu}$ = Умножаемъ числителя и знаменателя на $(m-\nu)!$ имѣемъ $\binom{m}{\nu} = \frac{m!}{\nu!\, (m-\nu)!}$ или $= \frac{(a+b)!}{a!\, b!}$. Всѣ простые множители знаменателя очевидно входятъ въ числитель; разсмотримъ показашее при одном из них, p; показатель при p в числителе есть $\sum\limits_{\nu=1,2\dots}\left[\frac{a+b}{p^\nu}\right]$, а в знаменателе $\sum\limits_{\nu=1,2\dots}\left[\frac{a}{p^\nu}\right]+\sum\limits_{\nu=1,2\dots}\left[\frac{b}{p^\nu}\right]=\sum\limits_{\nu=1,2\dots}\left(\left[\frac{a}{p^\nu}\right]+\left[\frac{b}{p^\nu}\right]\right)$

Докажем, что $\sum\left[\frac{a+b}{p^\nu}\right]\geqq\sum\left(\left[\frac{a}{p^\nu}\right]+\left[\frac{b}{p^\nu}\right]\right)$

Лемма. Дано $x>0$, $y>0$ – рацион. числа; тр. док. $[x+y]\geq[x]+[y]$.

Док. $x\geqq[x]$, $y\geqq[y]$; $x+y\geqq[x]+[y]$. Число $x+y$ больше или равно целому числу $[x]+[y]$, сл. и его целая часть $[x+y]\geq[x]+[y]$.

Применяя эту лемму к нашему случаю, имеем:

$$\left[\frac{a+b}{p^\nu}\right]\geqq\left[\frac{a}{p^\nu}\right]+\left[\frac{b}{p^\nu}\right],\ \text{значит}\ \sum_{\nu=1,2\dots}\left[\frac{a+b}{p^\nu}\right]\geqq\sum_{\nu=1,2\dots}\left(\left[\frac{a}{p^\nu}\right]+\left[\frac{b}{p^\nu}\right]\right)$$ что и тр. док.

Глава 3. Об общем наибольшем делителе и общем наименьшем кратном.

Имеем число $a=p_1^{\alpha_1}\dots p_s^{\alpha_s}$, где $\alpha_k\geqq1$.

Делитель d числа a не может иметь первоначальных множителей, отличных от p_k. Допустим обратное: $q\,|\,d$, где q простое число, отличное от p_k; получим ~~q a d e~~ $q\,|\,d\,|\,a$, т.е. в разложении a войдет простой множитель q, что невозможно.

Итак, каждый делитель d числа a имеет форму:

$$d=p_1^{\beta_1}\dots p_s^{\beta_s},\ \text{где}\ 0\leqq\beta_k\leqq\alpha_k.$$

Если бы имели, например $\beta_1>\alpha_1$, т.е. $\beta_1\geqq\alpha_1+1$, то имели бы $p_1^{\alpha_1+1}\,|\,d\,|\,a$. Тогда разложение a было бы $a=p_1^{\alpha_1+1}\cdot a_1$, что невозм

Итак $a = d \cdot p_1^{\alpha_1 - \beta_1} \ldots p_\rho^{\alpha_\rho - \beta_\rho}$.

β_1 может иметь ~~(в разных д.)~~ $\alpha_1 + 1$ значений $(0, 1, \ldots \alpha_1)$,

β_2 может принимать $\alpha_2 + 1$ значений, и т. д.; β_ρ $\alpha_\rho + 1$ значений.

Комбинируя в произведении разные показатели при первоначальных множителях, мы получим все возможные делители числа a; их число будет

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_\rho + 1)$$

Итак, число делителей данного числа зависит только от показателей при простых делителях в разложении этого числа.

2 числа a и b называются взаимно простыми, если они не имеют общего делителя, кроме 1.

Теорема. Дано: $p \nmid b$; тр. док.: p и b взаимно простые числа

Док. Допустим обратное: пусть p и b имеют общего делителя $d > 1$.

Тогда $d \mid p$, $d \mid b$; из $1^{го}$ заключаем $d = p$, откуда $p \mid b$, что невозможно.

Относительно простого числа p все числа можно разделить на 2 класса — делящиеся на него и не делящиеся

Пусть нам даны 2 числа:

$$a = p_1^{\alpha_1} \ldots p_\rho^{\alpha_\rho} \quad и \quad b = q_1^{\beta_1} \ldots q_\sigma^{\beta_\sigma}, \quad гдѣ\ \alpha_k > 0\ и\ \beta_k > 0.$$

Ищем их общие делители. Если, напр. $b = 1$, или всѣ q различны

от p, то единственный общий делитель $= 1$. Чтобы были общие делители a и b, отличные от 1, хоть одно из p должно быть равно наиб. d.
Введем новое обозначение разложений a и b

$$a = p_1^{\alpha_1} \ldots p_r^{\alpha_r} ; \; b = p_1^{\beta_1} \ldots p_r^{\beta_r} , \text{ где } \alpha, \beta \geqq 0, \text{ и}$$

никогда не бывает одновременно $\alpha_k = \beta_k = 0$. Тогда всякий общий делитель a и b будет иметь вид:

$$c = p_1^{\gamma_1} \ldots p_r^{\gamma_r} , \text{ где } \gamma_k \geqq 0 \text{ и } \gamma_k \leqq \alpha_k , \gamma_k \leqq \beta_k .$$

Введем обозначение: наименьшее из чисел $d_1, d_2, \ldots d_n$ будем обозначать $Min(d_1, d_2, \ldots d_n)$. Тогда γ_1 представится так:

$\gamma_1 \leqq Min(\alpha_1, \beta_1) = \delta_1$, т. е. $0 \leqq \gamma_1 \leqq \delta_1$. ~~Состав~~ $0 \leqq \gamma_2 \leqq \delta_2$ и т. д.
Составим выражение

$$p_1^{\delta_1} p_2^{\delta_2} \ldots p_r^{\delta_r} = d$$

Это будет определенное целое число, общий делитель чисел a и b. Если возьмем какой-нибудь общий делитель a и b, c, то очевидно $c \mid d$. d называется общим наибольшим делителем чисел a и b. Определив общий наиб. делитель, мы одновременно дали способ его нахождения путем разложения чисел на первонач. множители.
Приведем другой способ нахождения общего наиб. делителя.
Даны 2 числа a и a_1. Если $a = a_1$, то a и есть общ. наиб. делитель.
Пусть теперь $a > a_1$; $a = q_1 a_1 + a_2$, где $a_1 > a_2 \geqq 0$. Если $a_2 = 0$, то a_1 есть общ. наиб. делитель, если нет, продолжаем.

$a_1 = q_2 a_2 + a_3$, где $a_2 > a_3 \geqq 0$; если $a_3 \neq 0$, то идем дальше и т. д. Пусть наконец $a_{m-2} = q_{m-1} a_{m-1} + a_m$; $a_{m-1} = q_m a_m$. Тогда a_m есть общий наибольший делитель чисел a и a_1. Докажем, что a_m есть общий дел. a и a_1: из посл. равенства $a_m | a_{m-1}$, из предыдущего в связи с этим $a_m | a_{m-2}$ и т. д. дойдем до $a_m | a_1$ и $a_m | a$.
Чтобы показать, что a_m есть общий наиб. делитель a и a_1, покажем, что всякий общий делитель a и a_1, например $e | a_m$.
Мы имеем: $e | a$, $e | a_1$; из $1^{го}$ равенства следует, что $e | a_2$, из $2^{го}$ в связи с этим: $e | a_3$, и т. д. Наконец $e | a_{m-1}$, и $e | a_m$, что и тр. д.
Общий наиб. делитель a и b будем обозначать (a, b)

<u>Теорема</u>. Дано: $(a, b) = d$; тр. док. $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Доказ. Пусть $\left(\frac{a}{d}, \frac{b}{d}\right) = e$; тогда $e | \frac{a}{d}$, $e | \frac{b}{d}$; $de | a$, $de | b$. Если $e > 1$, то d не общий наибольший делитель, что противор. условию. Сл. $e = 1$.

<u>Обр. теорема</u>. Дано: $d | a$, $d | b$; $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Тр. док. $d = (a, b)$.
Доказ. Пусть $(a, b) = df$; $df | a$, $df | b$. Значит, $f | \frac{a}{d}$, $f | \frac{b}{d}$, сл. $f = 1$, $(a, b) = d$, что и тр. док.

Пусть дано несколько чисел:

$$a = p_1^{\alpha_1} \dots p_\tau^{\alpha_\tau}, \quad b = p_1^{\beta_1} \dots p_\tau^{\beta_\tau}, \quad c = p_1^{\gamma_1} \dots p_\tau^{\gamma_\tau}, \quad \dots$$

Составим число

$$d = p_1^{\delta_1} \dots p_\tau^{\delta_\tau}, \quad \text{где } \delta_\lambda = \min(\alpha_\lambda, \beta_\lambda, \gamma_\lambda, \dots), \quad \delta_\lambda \geqq 0.$$

d наибольший делитель; в с. д. докажем, что всякий общий делитель чисел $a, b, c, \dots$ делит d;

Дано: $e|a$, $e|b$, $e|c, \dots$ тр. док. $e|d$. Пусть показатель при p_1 в e есть ε_1; очевидно $\varepsilon_1 \leq \alpha_1$, $\varepsilon_1 \leq \beta_1$, $\varepsilon_1 \leq \gamma_1, \dots$, т.е. $\varepsilon_1 \leq \delta_1$; то же справедливо и относ. других показателей, итак $e|d$. $d = (a, b, c, \dots)$

Если $d = (a, b, c, \dots) = 1$, то числа $a, b, c, \dots$ наз. взаимно простыми.

О наименьшем общем кратном.

Пусть имеем числа:

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r} \quad \text{и} \quad b = p_1^{\beta_1} \dots p_r^{\beta_r}.$$

Пусть c обладает таким свойством, что $a|c$ и $b|c$. Тогда мы назовем c общим кратным a и b; общих кратных 2 чисел бесч. множество
напр. $c = ab$, $c = gab$, где g люб. целое число.

Введем обозначения $M_x(\alpha_1, \beta_1)$ есть наибольшее из чисел α_1 и β_1.
есть μ_1, и т.д.

~~Теорема~~ (Определение). Общее наим. кратное 2 чисел a и b делит всякое общее их кратное. Назовем: $\mathrm{Max}(\alpha_1, \beta_1) = \mu_1, \dots, \mathrm{Max}(\alpha_r, \beta_r) = \mu_r$.

Возьмем $m = p_1^{\mu_1} \dots p_r^{\mu_r}$; ясно, что $a|m$ и $b|m$ ($\alpha_1 \leq \mu_1$, $\beta_1 \leq \mu_1$, и т.д.)

Следов. m есть общее кратное; докажем, что оно наименьшее

Дано: $a|c$, $b|c$; тр. док. $m|c$. Разлагаем c на простые множители

Каждому простому множ. a и b соотв. тот же множитель в c в степени (по крайней мере) $= \mu$; значит $m|c$.

Теорема. Докажем, что $ab = md$; имеем $a = \prod p^{\alpha}$, $b = \prod p^{\beta}$;

$m = \prod p^{\max(\alpha,\beta)}$, $d = \prod p^{\min(\alpha,\beta)}$; $ab = \prod p^{\alpha+\beta}$; $md = \prod p^{\max(\alpha,\beta)+\min(\alpha,\beta)}$

Докажем, что $\max(\alpha,\beta) + \min(\alpha,\beta) = \alpha + \beta$. 1) $\alpha = \beta$, тогда $2\alpha = 2\alpha$
доказано

2) $\alpha>\beta$; $\max(\alpha,\beta)=\alpha$, $\min=\beta$; $\alpha+\beta=\alpha+\beta$; 3) $\alpha<\beta$; $\beta+\alpha=\alpha+\beta$.
Итак, $ab=md$.

Теорема. Дано: $(a,b)=1$; $a|c$, $b|c$; тр. док.: $ab|c$ — доказывается на основании пред., что ab есть наименьшее кр. a и b.

Пусть даны несколько чисел:

$$a=p_1^{\alpha_1}\dots p_r^{\alpha_r}\ ;\ b=p_1^{\beta_1}\dots p_r^{\beta_r}\ ;\ c=p_1^{\gamma_1}\dots p_r^{\gamma_r},\ \dots$$

Наименьшее кратное их,

$$m=p_1^{\max(\alpha_1,\beta_1,\gamma_1,\dots)}\dots p_r^{\max(\alpha_r,\beta_r,\gamma_r\dots)}$$

Всякое общее кратное чисел $a, b, c, \dots$ есть кратное m.

Теорема. Дано: $(a,n)=1$, $(b,n)=1$; тр. док. $(ab,n)=1$. Доказ. Пусть $p|n$, $p|ab$; значит или $p|a$ или $p|b$ — против условия.

Теорема. Дано $(a,n)=1$, $n|ab$; тр. док. $n|b$. Доказ. $n|ab$, $a|ab$; значит $na|ab$, т.е. $n|b$, что и тр. док.

Теорема: Дано $a=b^m$, $a=p_1^{\alpha_1}\dots p_\rho^{\alpha_\rho}$. Тр. доказать: $m|\alpha_1,\dots m|\alpha_\rho$. Доказ. $b=p_1^{\beta_1}\dots p_\rho^{\beta_\rho}$; $a=b^m=p_1^{m\beta_1}\dots p_\rho^{m\beta_\rho}$. Итак $\alpha_1=m\beta_1,\dots \alpha_\rho=m\beta_\rho$, т.е. $m|\alpha_1,\dots m|\alpha_\rho$, что и тр. док.

Теорема. Дано $(a,b)=1$, $ab=c^m$. Тр. док. $a=d^m$, $b=e^m$. Доказ.: $a=p_1^{\alpha_1}\dots p_\rho^{\alpha_\rho}$; $b=q_1^{\beta_1}\dots q_\sigma^{\beta_\sigma}$; $ab=p_1^{\alpha_1}\dots p_\rho^{\alpha_\rho}.q_1^{\beta_1}\dots q_\sigma^{\beta_\sigma}$. По предыдущему $m|\alpha_1,\dots m|\alpha_\rho$; $m|\beta_1,\dots m|\beta_\sigma$, т.е. a и b суть $m^{ые}$ степени целых чисел, что и тр. доказать.

Глава 4. О нѣкоторых числовых функціях.

Числовыми функціями ($y=f(n)$), называются такія, аргумент которых принимает только цѣлыя положительныя значенія.

С одной из таких функцій мы уже встрѣтились. Мы нашли формулу, дающую число дѣлителей данного числа
$$n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_\rho^{\alpha_\rho}.$$
Это было $T(n)=(\alpha_1+1)(\alpha_2+1)\dots(\alpha_\rho+1)$.

Найдем выраженіе другой числовой функціи $\sigma(n)$ - сумма всѣх дѣлителей данного числа. Легко видѣть, что
$$\sigma(n)=(1+p_1+\dots p_1^{\alpha_1})(1+p_2+\dots p_2^{\alpha_2})\dots(1+p_\rho+\dots+p_\rho^{\alpha_\rho}).$$
Замѣтив, что каждая скобка есть сумма геометрической прогрессіи, напишем эту же функцію в видѣ
$$\sigma(n)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\dots\frac{p_\rho^{\alpha_\rho+1}-1}{p_\rho-1}.$$
Выведем формулу произведенія всѣх дѣлителей данного числа. Пусть сначала n не квадратное число; если d дѣлитель числа n, то $\frac{n}{d}$ - другой дѣлитель. Т. обр. всѣ дѣлители располагаются в порядке, причем произведеніе каждой пары $=n$. Итак, произведеніе дѣлителей для всякаго не квадратнаго числа выразится формулой
$$n^{\frac{T(n)}{2}}$$

Если же n точный квадрат, то одному делителю, $\sqrt{n}$, не найдется парного, и произведение делителей представится в виде:

$$\sqrt{n}\cdot n^{\frac{T(n)-1}{2}} = n^{\frac{T(n)}{2}}$$

Очевидно, $T(n)$ ~~(может быть)~~ будет нечетным только в случае, если n есть точный квадрат.

Выводем некоторые свойства функции σ; т. к. $\sigma(p_\alpha^\alpha)=\frac{p^{\alpha+1}-1}{p-1}$, то для $\sigma(n)$ имеем выражение:

$$\sigma(n)=\sigma(p_1^{\alpha_1})\cdot\sigma(p_2^{\alpha_2})\dots\sigma(p_\rho^{\alpha_\rho}),$$ где все $p_1, p_2, \dots p_\rho$ различны.

Вообще, если $(a, b)=1$, то

$$\sigma(ab)=\sigma(a)\cdot\sigma(b).$$

~~Если мы~~ Формула суммы истинных делителей числа n (не считая самого n), есть

$$\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\dots\frac{p_\rho^{\alpha_\rho+1}-1}{p_\rho-1}-n=\sigma(n)-n.$$

К этой функции примыкает неразрешенная до сих пор задача: найти все числа, равные сумме своих истинных делителей. Такие числа называются совершенными; как примеры, укажем $6=1+2+3$; $28=1+2+4+7+14$.

Эта задача приводит к уравнению

$$\sigma(n)-n=n \quad \text{или} \quad \sigma(n)=2n \quad, \text{т. е.}$$

$$\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_s^{\alpha_s+1}-1}{p_s-1}=2p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}.$$

Различаем 2 случая: 1) для n нечетнаго; 2) для n четнаго.
Относительно 1 случая мы не знаем ничего, т. е. не знаем ни одного числа, удовлетворяющаго условію, и не можем доказать, что таких чисел не существует.
Разсмотрим подробнѣе 2ой случай, и четное
$n=2^\alpha\cdot b$, гдѣ $\alpha\ge1$, b — нечетное число. Подст. в уравненіе

$$\sigma(n)=2n;\quad \sigma(n)=\sigma(2^\alpha)\cdot\sigma(b);$$

$(2^{\alpha+1}-1)\,\sigma(b)=2^{\alpha+1}\cdot b$; $b\neq1$ *), слѣдовательно $b>1$.

$$\sigma(b)=\frac{2^{\alpha+1}\cdot b}{2^{\alpha+1}-1}=b+\frac{b}{2^{\alpha+1}-1}$$

Лѣвая часть и b цѣлыя числа, значит $2^{\alpha+1}-1\,|\,b$. Наше уравненіе можно представить в видѣ

$$\sigma(b)=b+b'$$

гдѣ $b'\,|\,b$ и $b'<b$ (b' есть цѣлая часть b).
$\sigma(b)$ есть сумма всѣх дѣлителей b; в правой части имѣем 2 дѣлителя b. Слѣд. b есть простое число, а $b'=1$. Тогда $n=2^\alpha(2^{\alpha+1}-1)$, гдѣ $\alpha>1$ и $2^{\alpha+1}-1$ — простое число. Это условіе необходимое, чтобы n было совершенным числом. Докажем, что оно и достаточно. Пусть $n=2^\alpha(2^{\alpha+1}-1)$, тогда $\sigma(n)=\sigma(2^\alpha)\cdot\sigma(2^{\alpha+1}-1)=(2^{\alpha+1}-1)\cdot2^{\alpha+1}=2n$.
Итак, всѣ совершенныя четныя числа даются формулой:

---

*) если $b=1$, то $n=2^\alpha$; $\sigma(n)=2^{\alpha+1}-1$, не удовлетворяет уравненію

и $2^{k-1}(2^k-1)$, где 2^k-1 простое число.

Этому условию удовлетворяют значения $k=2,3,5,7,13,17,19,31,61$...

Соответственные совершенные числа будут: 6, 28, 496, 8128, ...

Заметим, что для того, чтобы 2^k-1 было простым числом, необходимо, чтобы k было простым числом. Докажем теорему.

Дано: 2^k-1 — простое число; тр. док: k простое число. Основываемся на тождестве: $\frac{y^\nu-1}{y-1}=y^{\nu-1}+y^{\nu-2}+\dots+1$; пусть $y=x^s$; $\frac{x^{\nu s}-1}{x^s-1}=x^{s(\nu-1)}+x^{s(\nu-2)}+\dots+x^s+1$.

Если $x=2$, то $\frac{2^{\nu s}-1}{2^s-1}=g$ (пол. ц. число). Если бы k не было простым числом ($k=\nu\cdot s$), то имели бы: $2^s-1 \mid 2^{\nu s}-1$, т.е. 2^k-1 — не простое число.

До сих пор не доказано, существует ли бесконечное множество чисел простых вида 2^k-1.

Решим другую задачу: определить все числа, произведение истинных делителей которых равно самому числу.

Получаем уравнение: $a=\frac{a^{\frac{1}{2}\tau(a)}}{a}$ или $a^2=a^{\frac{1}{2}\tau(a)}$, откуда $\tau(a)=4$. ~~Имеем~~ Пусть $a=p_1^{\alpha_1}\dots p_s^{\alpha_s}$; тогда $\tau(a)=(\alpha_1+1)\dots(\alpha_s+1)=4$.

4 можно представить в виде произведения двояко: $4=4$ и $4=2\cdot 2$.

Первому способу соответствуют решения $a=p^3$ (p любое простое число).

Второму случаю соответствует: $a=pq$ (p и q — 2 любых простых числа).

Рассмотрим Эйлерову числовую функцию $\varphi(n)$, выражающую число чисел, меньших n и взаимно с ним простых.

Если данное число простое, p, то очевидно $\varphi(p) = p-1 = p\left(1-\frac{1}{p}\right)$. Пусть теперь $n = p^\lambda$; тогда

$$\varphi(p^\lambda) = p^\lambda - p^{\lambda-1} = p^\lambda\left(1-\frac{1}{p}\right) = n\left(1-\frac{1}{p}\right)$$

Пусть теперь $n = p^\alpha q^\beta$, где $p \neq q$, $\alpha \geqq 1$, $\beta \geqq 1$. Тогда

$$\varphi(n) = \varphi(p^\alpha q^\beta) = p^\alpha q^\beta - \text{число ~~составных~~ чисел, делящихся на } p \text{ или } q.$$

Число чисел, меньших n и делящихся на p есть $\frac{n}{p}$, меньших n и делящихся на q $\frac{n}{q}$; если бы мы только вычли из n $\frac{n}{p}$ и $\frac{n}{q}$, то оказалось, что числа, делящиеся на pq, вычтены 2 раза; чтобы получить $\varphi(n)$, надо прибавить их число, равное $\frac{n}{pq}$. Получим:

$$\varphi(n) = n - \frac{n}{p} - \frac{n}{q} + \frac{n}{pq} = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right).$$

Пусть теперь

$$n = p^\alpha q^\beta r^\gamma.$$

$\varphi(n) = n -$ число чисел кратных $p -$ ч. кр. $q -$ ч. кр. $r +$ ч. кр. $pq +$ ч. кр. $pr +$ ч. кр. $qr -$ ч. кр. $pqr =$

$$= n - \frac{n}{p} - \frac{n}{q} - \frac{n}{r} + \frac{n}{pq} + \frac{n}{pr} + \frac{n}{qr} - \frac{n}{pqr} = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)$$

Пусть вообще

$$n = p_1^{\alpha_1} \dots p_\rho^{\alpha_\rho}.$$

Докажем, что в этом случае будет справедлива формула

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_\rho}\right) = p_1^{\alpha_1-1}(p_1-1)\dots p_\rho^{\alpha_\rho-1}(p_\rho-1)$$

Раскроем правую часть этой формулы:

$$\varphi(n) = n - \sum\frac{n}{p_1} + \sum\frac{n}{p_1p_2} - \sum\frac{n}{p_1p_2p_3} + \dots + (-1)^\sigma\sum\frac{n}{p_1p_2\dots p_\sigma} + \dots + (-1)^\rho\frac{n}{p_1p_2\dots p_\rho}$$

Заметим, что числа членов (слагаемых) (суммах) правой части будут соответственно равны:

$$1, \ \rho, \ \binom{\rho}{2}, \ \binom{\rho}{3}, \dots \binom{\rho}{\sigma}, \dots \ 1.$$

а общее число членов есть 2^ρ.

Докажем, что в написанном выражении $\varphi(n)$ всякое число $< n$ и взаимно с ним простое сосчитано 1 раз, а не вз. простое с n сосчитано 0 раз.*) Возьмем число, меньшее n и делящееся на $p_1, p_2, \dots p_\sigma$. Оно будет сосчитано в n один раз, в $\sum \frac{n}{p_1}$ σ раз, в $\sum \frac{n}{p_1 p_2}$ $\binom{\sigma}{2}$ раз, в $\sum \frac{n}{p_1 p_2 p_3}$ $\binom{\sigma}{3}$ раз, и т. д., в $\sum \frac{n}{p_1 p_2 \dots p_\sigma}$ $\binom{\sigma}{\sigma} = 1$ раз. (Следовательно) дальше не будет; Следовательно всего оно сосчитано

$$1 - \sigma + \binom{\sigma}{2} - \binom{\sigma}{3} + \dots + (-1)^\sigma \cdot 1 = (1-1)^\sigma = 0.$$

Итак, справедливость формулы для $\varphi(n)$ нами доказана.

Сокращенно можно обозначить:

$$\varphi(n) = n \prod \left(1 - \frac{1}{p}\right) = \prod p^{\alpha-1}(p-1).$$

Заметим, что $\varphi(n)$ всегда четно для $n \geqq 3$, т. к. для простых чисел, кроме 2, $p-1$ четно, а для степеней двух $\varphi(2^\alpha) = 2^{\alpha-1}$ четное при $\alpha > 1$. К тому же выводу придем из других соображений: Если $1 \leqq k \leqq \frac{n}{2}$ и если k взаимно простое с n число, то и $n-k$

---

*) Если число, меньшее n, взаимно простое с ним, то оно будет сосчитано в n 1 раз и больше нигде — в формуле $\varphi(n)$ · 1 раз. всего будет сосчитано

взаимно простое с n. Допустим, что это неверно: пусть $d \mid n-k$, $d \mid n$; но тогда $d \mid k$, т. е. $n-k$ и k не взаимно просты.
Итак, все взаимно простые с n числа располагаются в пары, и их число очевидно четное (если n четное, то для $k = \frac{n}{2}$ $n-k = \frac{n}{2}$, пары не получается, но $\frac{n}{2}$ есть делитель n).
Теорема. Дано $(a, b) = 1$. Тр. док. $\varphi(a.b) = \varphi(a).\varphi(b)$.
Пусть $a = \prod p^\alpha$, $b = \prod q^\beta$; $\varphi(a) = \prod \varphi(p^\alpha)$, $\varphi(b) = \prod \varphi(q^\beta)$;
$\varphi(a).\varphi(b) = \prod \varphi(r^\gamma)$, где r суть все p и q, γ суть соответственные показатели α и β. Но, с другой стороны $\varphi(a.b) = \prod \varphi(r^\gamma)$, т. е. $\varphi(a.b) = \varphi(a).\varphi(b)$, что и тр. док.
Теорема (Гаусса); дано число m; ~~будет~~ пусть d — его делитель. Тр. док. $\sum_{d/m} \varphi(d) = m$. Доказательство: 1 случай: $m = p^\alpha$;

$$\sum_{d/m} \varphi(d) = \varphi(1) + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^\alpha) = 1 + (-1+p) + (-p+p^2) + \ldots + (-p^{\alpha-1} + p^\alpha) = p^\alpha = m.$$

2 случай. Пусть вообще $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots$

$$\sum_{d/m} \varphi(d) = [1 + \varphi(p_1) + \varphi(p_1^2) + \ldots + \varphi(p_1^{\alpha_1})][1 + \varphi(p_2) + \varphi(p_2^2) + \ldots + \varphi(p_2^{\alpha_2})][\ldots]\ldots$$

В справедливости этого равенства убедимся, раскрывая скобки и применяя предыдущую теорему; ~~получаем~~ получаем.

$$\sum_{d/m} \varphi(d) = p_1^{\alpha_1}.p_2^{\alpha_2}\ldots = m$$

Другое доказательство той же теоремы. Пусть дано число m; рассмотрим числа $1, 2, 3, \ldots m$, количество их m. Очевидно это

как m — числу чисел взаимно простых с m + число чисел, не взаимно простых с m.
Числа, не взаимно простые с m, имеют с ним общаго наибольшаго дѣлителя $d>1$. Итак

$$m=\varphi(m) + \text{число чисел, не взаимно простых с } m.$$

Пусть $d \mid m$; найдем всѣ числа n, удовлетворяющія условію: $(m,n)=d$, гдѣ $1 \leqq n \leqq m$.
Числа, меньшія или равныя m и кратныя d суть:

$$1.d\ ,\ 2.d\ ,\ \ldots\ \frac{m}{d}d.$$

Возьмем какое-нибудь из них, xd, гдѣ $1 \leqq xd \leqq m$, ~~и удова оно удовлетворяет~~ и удовлетворяющее условію:

$$(xd, m)=d \quad \text{или} \quad (xd, \tfrac{m}{d}d)=d.$$

На основаніи предыдущаго

$$(x, \tfrac{m}{d}) = 1.$$

Очевидно, x есть число взаимно простое с $\frac{m}{d}$; число таких чисел есть $\varphi(\frac{m}{d})$. Итак

$$m=\varphi(m)+\sum_{d|m,\,d>1}\varphi\left(\frac{m}{d}\right)$$

Замѣтим, что при $d=1$ $\varphi(\frac{m}{d})=\varphi(m)$. Наша формула запишется так: $m=\sum_{d|m}\varphi(\frac{m}{d})$, считая сумму распространенной на всѣ $d|m$, включая 1. Так как при всевозможных значеніях d мы получим от дѣленія m на d всѣ дѣлители числа m, то, переставляя порядок слагаемых можем написать:

$$m = \sum_{d/m} \varphi(d).$$

Это свойство характеристическое для функции φ: если существует такая функция ψ, что для нея всегда имеет место равенство: $\sum_{d/m} \psi(d) = m$, то ~~невып~~ $\psi \equiv \varphi$.

В самом деле: $\psi(1) = 1 = \varphi(1)$; $\psi(1)+\psi(2) = 2 = \varphi(1)+\varphi(2)$, т. е. $\psi(2)=\varphi(2)$, и так далее — докажем, что для всякого m $\psi(m) = \varphi(m)$.

Введем числовую функцию $\mu(m)$ (Mertens'a), которая определяется как: 1) $\mu(1) = 1$; 2) $\mu(m) = 0$, если m содержит какой-либо простой множитель больше одного раза (т. е. ~~или~~ содержит в числе своих делителей квадратное число).

3) $\mu(m) = (-1)^s$, если $m = p_1 \dots p_s$, и все p различны между собой.

Приведем значения функции μ для чисел первого десятка:

$\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, $\mu(7) = -1$, $\mu(8) = 0$, $\mu(9) = 0$, $\mu(10) = 1$.

Докажем тожество:

$$\sum_{d/m} \mu(d) = \begin{cases} 1, & \text{если } m = 1 \\ 0, & \text{если } m > 1. \end{cases}$$

1ая часть утверждения очевидна; пусть теперь $m > 1$.

Рассмотрим случай: $m = p$ (простое число). Имеем:

$$\sum_{d/p} \mu(d) = \mu(1) + \mu(p) = 1 - 1 = 0.$$

Пусть затем $m = p^\alpha$. Тогда

$$\sum_{d/p^\alpha} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \dots \mu(p^\alpha) = 1 - 1 + 0 + 0 + \dots + 0 = 0.$$

Перейдем к общему случаю:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\rho^{\alpha_\rho}$$

Рассматривая делителей данного числа, мы сначала отбросим тѣ, кот. дѣлятся на квадратное число, т. к. в этом случаѣ $\mu(d) = 0$. Остальные дѣлители будут слѣдующих типов: $1, p, pq, pqr, \dots$ Соотвѣтствующие значения функции μ будут $1, -1, +1, -1, \dots$ (Подсчитывая) число дѣлителей каждаго типа будет соотвѣтственно:

$1, \binom{\rho}{1}, \binom{\rho}{2}, \binom{\rho}{3}, \dots$ Итак

$$\sum_{d/m} \mu(d) = 1 - \rho + \binom{\rho}{2} - \binom{\rho}{3} + \dots = (1-1)^\rho = 0.$$

Замѣтим, что выведенное свойство - характеристическое для функции μ; доказательство ведется таким же образом, как доказательство подобнаго свойства функции φ.

<u>Теорема</u>: Если $(m, n) = 1$, то $\mu(m.n) = \mu(m) \cdot \mu(n)$. Доказательство.

1) Если m или n или оба дѣлятся на квадрат, то в обѣих частях предполагаемаго равенства имѣем 0, оно справедливо.

2) m и n оба не дѣлятся на квадратные числа; пусть.

$m = p_1 p_2 \dots p_\rho$, $n = q_1 q_2 \dots q_\sigma$, гдѣ ни одно p не равно q.

Имѣем $mn = p_1 p_2 \dots p_\rho \cdot q_1 \cdot q_2 \dots q_\sigma$; $\mu(m.n) = (-1)^{\rho+\sigma}$, $\mu(m) = (-1)^\rho$; $\mu(n) = (-1)^\sigma$.

Равенство справедливо и в этом случаѣ. Теорема доказана

Пусть имеем любую числовую функцию $\Phi(m)$; можно получить одну и только одну числовую функцию $F(m)$, определяемую равенством: $F(m) = \sum_{d|m} \Phi(d)$.

Обратно, если дана в этом соотношении функция $F(m)$, то функция $\Phi(m)$ тоже вполне определена, в самом деле, имеем: $F(1) = \Phi(1)$; $F(2) = \Phi(1) + \Phi(2)$, т.е. $\Phi(2) = F(2) - F(1)$; $F(3) = \Phi(1) + \Phi(3)$, т.е. $\Phi(3) = F(3) - F(1)$ и т.д. Для простого числа p $\Phi(1) + \Phi(p) = F(p)$, т.е. $\Phi(p) = F(p) - F(1)$. Затем можно найти значения Φ и для составных чисел.

Зависимость между Φ и F выражается формулой:

$$\Phi(m) = \sum_{d|m} \mu(d) F\left(\frac{m}{d}\right), \quad \text{если } \sum_{d|n} \Phi(d) = F(n).$$

Пусть n - любой делитель числа m; $n|m$, $n = \frac{m}{\delta}$, т.е. $\delta|m$. Тогда $F\left(\frac{m}{\delta}\right) = \sum_{d|\frac{m}{\delta}} \Phi(d)$. Умножаем объ части на $\mu(\delta)$ и суммируем по всем $\delta|m$. Имеем:

$$\sum_{\delta|m} \mu(\delta) F\left(\frac{m}{\delta}\right) = \sum_{\delta|m} \mu(\delta) \sum_{d|\frac{m}{\delta}} \Phi(d) = \sum_{\delta|m} \sum_{d|\frac{m}{\delta}} \mu(\delta) \Phi(d).$$

Имеем $d|\frac{m}{\delta}$, т. $d\delta = D|m$, след. $d\delta|m$, $\delta|\frac{m}{d}$. Двойную сумму в правой части можно переписать:

$$\sum_{\delta|m} \sum_{d|\frac{m}{\delta}} \mu(\delta) \Phi(d) = \sum_{\substack{\delta d|m \\ \delta, d}} \mu(\delta) \Phi(d) = \sum_{d|m} \sum_{\delta|\frac{m}{d}} \mu(\delta) \cdot \Phi(d) =$$

$$= \sum_{d|m} \Phi(d) \cdot \sum_{\delta|\frac{m}{d}} \mu(\delta).$$ Все слагаемые внутренней суммы равны 0, кроме того, кот. соответствует $d = m$; он равен 1. Итак, имеем

$$\sum_{\delta/m}{}' \mu(\delta) F\left(\frac{m}{\delta}\right) = \Phi(m).,$$ что и тр. док.

Мы раньше имели:

$$\sum_{d/m}{}' \varphi(d) = m$$; по настоящей теореме

$$\varphi(m) = \sum_{d/m}{}' \mu(d) \frac{m}{d} = m \sum_{d/m}{}' \frac{\mu(d)}{d}.$$

2

Пусть имеем целое число $x \geq 1$. Тогда Докажем, что

$$\sum_{n=1}^{x}{}' \mu(n)\left[\frac{x}{n}\right] = 1.$$

Для $x=1$ имеем: $\mu(1)\left[\frac{1}{1}\right] = 1$; $x=2$; $\mu(1).\left[\frac{2}{1}\right] + \mu(2)\left[\frac{2}{2}\right] = 2-1=1$;

$x=3$; $\mu(1)\left[\frac{3}{1}\right] + \mu(2)\left[\frac{3}{2}\right] + \mu(3)\left[\frac{3}{3}\right] = 3-1-1 = 1$ и т. д.

Докажем справедливость этой формулы. Нам известно, что

$$\sum_{n/m}{}' \mu(n) = \begin{cases} 1 & \text{для } m=1 \\ 0 & \text{для } m>1. \end{cases}$$

Суммируем эту формулу по m от 1 до x.

$$\sum_{m=1}^{x}{}' \sum_{n/m}{}' \mu(n) = 1.$$

Суммировани распространяется на все числа от 1 до x и на все их делители; какой-нибудь делитель $n \leq x$ входит в эту сумму $\left[\frac{x}{n}\right]$ раз. Итак, имеем:

$$\sum_{n=1}^{x}{}' \mu(n)\left[\frac{x}{n}\right] = 1,$$ что и тр. док. (Бугаев)

Возьмем разность:

$$\sum_{n=1}^{x}{}' \mu(n)\frac{x}{n} - \sum_{n=1}^{x}{}' \mu(n)\left[\frac{x}{n}\right] = \sum_{n=1}^{x}{}' \mu(n)\frac{x}{n} - 1 =$$

$$= \sum_{n=1}^{x}{}' \mu(n)\left(\frac{x}{n} - \left[\frac{x}{n}\right]\right)$$; в последнюю сумму входит x членов, и

каждый изъ нихъ меньше 1 по абсолютному значенію; одинъ изъ членовъ навѣрно = 0, именно тотъ, в которомъ $n = x$

Итакъ $\left|\sum_{n=1}^{x}\mu(n)\frac{x}{n}-1\right| \leqq x-1$, откуда $\left|\sum_{n=1}^{x}\mu(n)\frac{x}{n}\right| \leqq x$.

Дѣлимъ обѣ части на x; получаемъ:

$$\left|\sum_{n=1}^{x}\frac{\mu(n)}{n}\right| \leqq 1.$$

Разсмотримъ рядъ: $\sum_{n=1}^{\infty}\frac{\mu(n)}{n}$. Предыдущая формула показываетъ, что сумма конечнаго числа членовъ этого ряда заключена в предѣлахъ $-1 \ldots +1$; но она еще ничего не говоритъ о сходимости этого ряда.

Сходимость этого ряда $1-\frac{1}{2}-\frac{1}{3}-\frac{1}{5}+\frac{1}{6}-\frac{1}{7}+\frac{1}{10}-\ldots$ доказана [illegible] в 1892 г.

Упомянемъ еще объ одной числовой функціи $\pi(x)$; она выражаетъ число простыхъ чиселъ, меньшихъ или равныхъ x; изъ предыдущаго слѣдуетъ, что при безконечно большомъ x $\pi(x)$ безконечно велика; можно доказать равенство:

$$\lim_{x=\infty}\frac{\pi(x)}{\frac{x}{\lg x}} = 1;$$

Эта формула выведена Hadamard'омъ и de la Vallée Poussin'омъ (1896).

Разность $\pi(x)-\frac{x}{\lg x}=F$ есть ошибка, которую мы дѣлаемъ, принимая для конечныхъ значеній x вмѣсто $\pi(x)$ $\frac{x}{\lg x}$; на основаніи приведенной формулы имѣемъ: $\lim_{x=\infty}\frac{\pi}{\pi-F}=1=\lim_{x=\infty}\frac{1}{1-\frac{F}{\pi}}$, т.е. $\lim_{x=\infty}\frac{F}{\pi}=0$.

Глава 5. О сравненіях.

Если даны 2 положит. целых числа a и m, то мы имеем соотношение

$$a = qm + r \quad , \text{ где } 0 \leq r \leq m-1.$$

Легко распространить это равенство на отрицательные значения a (тогда и q будет получать отриц. значения).

Пусть даны 3 числа: a, b и m, a и b — любые целые числа, m — целое положительное число. Условимся называть a и b сравнимыми по модулю m, если при делении на m они дают одинаковый остаток. Пусть (например) $a = qm + r$, $b = q_1 m + r$, ~~тогда~~, где $0 \leq r \leq m-1$; тогда пишем:

$$a \equiv b \pmod{m}$$

Можно придать определению другую форму; вычитаем b из a; имеем: $a - b = (q - q_1)m$, т.е. $m \mid a-b$.

Итак, если $a \equiv b \pmod{m}$, то $m \mid a-b$.

Докажем обратное положение: пусть $m \mid a-b$, $a = b + km$; если $a = mq + r$, то $b = a - km = (q-k)m + r$; итак $a \equiv b \pmod{m}$.

Следовательно, $a \equiv b \pmod{m}$, значит $m \mid a-b$.

Теорема. 1) $a \equiv a \pmod{m}$, потому что $m \mid a-a$

2) Если $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$. Доказ. $m \mid a-b$, $m \mid b-c$; m делит их сумму: $m \mid a-b+b-c$, $m \mid a-c$.

3) Если $a \equiv b \pmod m$, то $b \equiv a \pmod m$. Доказ.: если $m \mid a-b$, слѣд. $m \mid b-a$.

Дѣйствія над сравненіями.

I. Сложеніе и вычитанія сравненій; Теорема; дано: $a \equiv b$, $c \equiv d \pmod m$; тр. док. $a \pm c \equiv b \pm d \pmod m$. Доказ. $m \mid a-b$, $m \mid c-d$, слѣд. $m \mid a-b \pm c \mp d$ или $m \mid (a \pm c)-(b \pm d)$.

Теорема. Дано: $a_1 \equiv b_1, a_2 \equiv b_2, \dots a_\nu \equiv b_\nu \pmod m$. Тр. док.: $a_1+a_2+\dots+a_\nu \equiv b_1+b_2+\dots+b_\nu \pmod m$. Доказ. основывается на предыдущей теоремѣ.

II Умноженіе. Теорема. Дано: $a \equiv b \pmod m$; ν - любое цѣлое пол. число. тр. док.: $a\nu \equiv b\nu \pmod m$. Положим в предыдущей теоремѣ $a_1=a_2=\dots=a_\nu$ и $b_1=b_2=\dots=b_\nu$, имѣем $\nu a \equiv \nu b \pmod m$.

Теорема: дано $a \equiv b \pmod m$; тр. док. $-a \equiv -b \pmod m$. Доказ. очевидно.
Значит, обѣ части сравненія можно умножать на любое цѣлое число.

Теорема. Дано: $a \equiv b \pmod m$, $c \equiv d \pmod m$; треб. док. $ac \equiv bd \pmod m$. Доказательство: $a = b + qm$, $c = d + hm$. перемножаем эти равенства:

$$ac = bd + bhm + dqm + qhm^2 = bd + Mm.$$

2ое доказательство: умножаем 1ое сравненіе на c, а 2ое на b. $ac \equiv bc \pmod m$, $bc \equiv bd \pmod m$, слѣд. $ac \equiv bd \pmod m$.

УПОТРЕБИТЬ ВМѢСТО ПРОПУ… СКА

МЮРЪ и МЕРИЛИЗЪ,

МОСКВА.

ОТДѢЛЕНІЕ

ПИСЬМЕННЫХЪ и ЧЕРТЕЖНЫХЪ

ПРИНАДЛЕЖНОСТЕЙ.

МАСЛЯНЫЯ КРАСКИ

и

ПРИНАДЛЕЖНОСТИ ДЛЯ ЖИВОПИСИ.

БРОНЗА, ПОРТФЕЛИ, РАМКИ, СТЕРЕОСКОПЫ

и

ПРЕДМЕТЫ для ПОДАРКОВЪ.

МАТЕРІАЛЫ для ПЕРЕПЛЕТЧИКОВЪ,

футлярщиковъ и картонщиковъ.

ПРІЕМЪ ЗАКАЗОВЪ

НА ТИПО - ЛИТОГРАФСКІЯ РАБОТЫ.

ТИПОГРАФІЯ МЮРЪ и МЕРИЛИЗЪ.

Тетради ученическія,

съ листомъ пропускной бумаги въ каждой, изъ лучшей рижской бумаги, форматъ 1/4 листа писчей бумаги, въ толстой синей или коричневой обложкѣ.

съ фирм. **Мюръ и Мерилизъ.**

				За 1000 шт.	За дюж.	За шт.
№ 200.	Безъ линеекъ	въ	36 стран.	35 р.	45 к.	04 к.
„ 201.	Съ двойными узкими линейк. и промежут.	„	36 „	35 „	45 „	04 „
„ 202.	„ „ средними	„	36 „	35 „	45 „	04 „
„ 203.	„ „ широкими	„	36 „	35 „	45 „	04 „
„ 209.	„ 12 „ линіями безъ промежуточн.	„	36 „	35 „	45 „	04 „
„ 210.	„ 13 „ „ „	„	36 „	35 „	45 „	04 „
„ 211.	„ 14 „ „ „	„	36 „	35 „	45 „	04 „
„ 250.	„ 19 „ „ „	„	36 „	35 „	45 „	04 „
„ 204.	„ 23 одинарными линейками	„	36 „	35 „	45 „	04 „
„ 205.	„ 16 „ „	„	36 „	35 „	45 „	04 „
„ 206.	„ обыкновенными клѣтками	„	35 „	35 „	45 „	04 „
„ 206½	„ крупными клѣтками для ариѳметики	„	36 „	35 „	45 „	04 „
„ 216.	„ длинноватыми клѣтками	„	36 „	35 „	45 „	04 „
„ 207.	„ 3-мя лин. прям. и косыми	„	32 „	35 „	45 „	04 „
„ 208.	„ 2-мя „ „ „ „ и промежут.	„	32 „	35 „	45 „	04 „
„ 218.	„ 2-мя „ „ „ „ безъ промеж.	„	32 „	35 „	45 „	04 „
„ 228.	„ 2-мя „ „ „ „	„	32 „	35 „	45 „	04 „
„ 207½	„ 3-мя „ „ „ продольными	„	36 „	35 „	45 „	04 „
„ 227.	„ 2-мя „ „ „ „	„	36 „	35 „	45 „	04 „
„ 226.	„ длинноватыми клѣтками для письма	„	36 „	35 „	45 „	04 „
				За 100 штукъ.		
„ **217.**	Большой форматъ (цѣлый листъ), для каллиграфіи, съ тройн. прям. и косыми линіями	„	56 „	6 р. 30 к.	— „	07 „

Дано: $a_1 \equiv b_1, \dots, a_\nu \equiv b_\nu \pmod m$, тогда, на осн. предыдущаго
$$a_1 \dots a_\nu \equiv b_1 \dots b_\nu \pmod m.$$
Теорема: дано $a \equiv b \pmod m$; тр. док. $a^\nu \equiv b^\nu \pmod m$. Для доказ. полагаем в предыдущей формулѣ $a_1 = \dots = a_\nu = a$ и $b_1 = \dots = b_\nu = b$. (ν, конечно, цѣлое положит. число).

Выраженіе $f(x) = c_0 x^n + c_1 x^{n-1} + \dots + c_n$, гдѣ всѣ c — цѣлыя числа, называется цѣлой цѣлочисленной функціей.

Теорема. Дано: $a \equiv b \pmod m$. Тр. док. $f(a) \equiv f(b) \pmod m$.

Для доказательства замѣтим, что над ~~частями~~ обѣими частями даннаго сравненія производятся только дѣйствія возведенія в цѣлую пол. степень, умноженія и сложенія.

Дѣленіе сравненій.

Теорема. Дано: $\alpha k \equiv \beta k \pmod m$ и $(k, m) = 1$ и $k > 0$. Тр. док. $\alpha \equiv \beta \pmod m$.

Доказ. Имѣем: $m \mid \alpha k - \beta k = k(\alpha - \beta)$. Т. к. $(k, m) = 1$, то $m \mid \alpha - \beta$.

Пусть теперь $(k, m) = \delta$; $m \mid \alpha k - \beta k$, т. е. $\frac{m}{\delta}\delta \mid \frac{k}{\delta}\delta(\alpha - \beta)$, слѣдовательно $\frac{m}{\delta} \mid \frac{k}{\delta}(\alpha - \beta)$; т. к. $\left(\frac{m}{\delta}, \frac{k}{\delta}\right) = 1$, то $\frac{m}{\delta} \mid \alpha - \beta$. Итак, в этом случаѣ
$$\alpha \equiv \beta \left(\mathrm{mod}\ \frac{m}{\delta}\right)$$
Итак, вообще, если $\alpha k \equiv \beta k \pmod m$, то $\alpha \equiv \beta \left(\mathrm{mod}\ \frac{m}{(m,k)}\right)$

Приведенныя правила можно примѣнять и на случаи отрицательнаго k, условившись считать $(u, v) = (|u|, |v|)$, если $u \gtrless 0$, $v \gtrless 0$

Теорема. Дано: $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$ ... $a \equiv b \pmod{m_\nu}$

Тр. док. $a \equiv b \pmod{M}$, где M = наим. кратное чисел $m_1, m_2, .. m_\nu$.

Доказ.: $m_1 | a-b$, $m_2 | a-b$, ... $m_\nu | a-b$, сл. $M | a-b$.

Теорема. Дано $a \equiv b \pmod{m}$. Тр. док. $(a, m) = (b, m)$. Доказ.

пусть $(a, m) = d$; $\overset{\text{по дан.}}{a = b + wm}$; $d | a$, $d | m$, след. $d | b$. Допустим, что $(b, m) = e$; e есть делитель a, но $d | a$, след. $e = d$

Следствие: $a \equiv b \pmod{m}$, $(a, m) = 1$. Тогда $(b, m) = 1$.

Приложение: признак делимости на 9 в десятичной системе:

$$N = c_0 10^m + c_1 10^{m-1} + \ldots + c_m, \text{ где } 0 \leq c \leq 9.$$

$10 \equiv 1 \pmod 9$, сл. $f(10) \equiv f(1) \pmod 9$, т. е. $N \equiv c_0 + c_1 + \ldots + c_m \pmod 9$.

Признак делимости на 11.

$10 \equiv -1 \pmod{11}$, сл. $f(10) \equiv f(-1) \pmod{11}$, т. е.

$$N \equiv (-1)^m c_0 + (-1)^{m-1} c_1 + \ldots \mp c_{m-1} + c_m \pmod{11}.$$

Пусть m – любое целое положительное число.

Полной системой вычетов по модулю m называется система m чисел, которые сравнимы с $0, 1, \ldots m-1$ по модулю m. Таковы, например, системы:

$$0, 1, 2, \ldots, m-1 \quad \text{или} \quad 0, -1, -2, \ldots, -(m-1).$$

Теорема. Если имеем m чисел, из которых любые 2 не сравнимы $\pmod{m}$, то они образуют полную систему вычетов по модулю m.

Доказ. $a = qm + r$, $b = q_1 m + r_1$. Если $a \not\equiv b \pmod{m}$, то $r \neq r_1$. Все различные значения r суть: $0, 1, 2, \ldots, m-1$, числом m; след. наша система исчерпает все эти значения. т. е. $a \equiv r \pmod m$

<u>Теорема.</u> За полную систему вычетов $(\mathrm{mod}\ m)$ можно принять систему: $a, a+1, a+2, \ldots, a+m-1$, где a — любое целое число.
Допустим, что $a+\lambda \equiv a+\lambda' \pmod m$, тогда $\lambda \equiv \lambda' \pmod m$, $m \mid \lambda-\lambda'$, что невозможно. Теорема доказана.

Всякое число сравнимо $(\mathrm{mod}\ m)$ с одним и только с одним из чисел полной системы вычетов; т. обр. все числа по отношению к m разбиваются на m классов: все числа одного и того же класса сравнимы с одним и тем же числом системы выч. $(\mathrm{mod}\ m)$.
Из числа m классов, на кот. разбиваются по отношению к m все числа, $\varphi(m)$ классов будут обладать тем свойством, что все заключающиеся в них числа взаимно просты с m.

<u>Теорема.</u> Дано $(k, m) = 1$. Тр. док. числа $0, k, 1.k, 2.k, \ldots (m-1).k$ образуют полную систему вычетов $(\mathrm{mod}\ m)$. Доказат.: допустим, что $\alpha k \equiv \beta k \pmod m$, где $\alpha \neq \beta$, и $\alpha, \beta = 0, 1, \ldots, m-1$ тогда $\alpha \equiv \beta \ (\mathrm{mod.}\ m)$, а это невозможно.

<u>Теорема.</u> Дано: $(k, m) = 1$; $b_1, b_2, \ldots b_m$ — полная система вычетов $(\mathrm{mod}\ m)$. Тр. док. $b_1k, b_2k, \ldots, b_mk$ тоже образуют полную систему вычетов $(\mathrm{mod}\ m)$. Доказ. Допустим, что $bk \equiv b'k \pmod m$, тогда $b \equiv b' \pmod m$, что противоречит данным.

О решении сравнений.

Теорема. Если сравнение имеет $kx \equiv c \pmod m$, где x — неизвестное целое число и $(k, m) = 1$, то это сравнение имеет решение (и притом (mod m) одно); в самом деле, это будет одно из решений чисел в предыдущей теореме. Назовем это решение x_0; тогда все остальные решения сравнения будут даны формулой

$$x = x_0 + \lambda m, \text{ где } \lambda \text{ — любое целое число,}$$

В самом деле $kx = kx_0 + k\lambda m \equiv kx_0 \equiv c \pmod m$.

Все корни, сравнимые с $x_0 \pmod m$, считаем за одно решение.

Сравнение $kx \equiv c \pmod m$ имеет только один корень, т.к. в полной системе ~~из~~ вычетов ~~остатков~~ $0 \cdot k, 1 \cdot k, 2 \cdot k, \ldots (m-1)k$ есть только один, сравнимый с $c \pmod m$.

Другое док. Пусть сущ. 2 корня: $kx_1 \equiv c \pmod m$, $kx_2 \equiv c \pmod m$, сл. $k(x_1 - x_2) \equiv 0 \pmod m$, т. е. $x_1 - x_2 \equiv 0 \pmod m$, $x_1 \equiv x_2 \pmod m$, x_2 и x_1 заключаются в одной формуле, ~~а не две другого корня~~ и т.д.

Перейдем к общему случаю. Дано сравнение

$$kx + l \equiv 0 \pmod m,$$

причем $(k, m) = d$. Это сравнение равносильно неопределенному уравнению $kx + l = my$. Для возможности решения необходимо, чтобы $d \mid l$. Докажем, что это условие и достаточно. Делим обе части сравнения и модуль на d (на осн. одной из пред. теор.)

Имѣем: $\frac{k}{d}x + \frac{l}{d} \equiv 0 \pmod{\frac{m}{d}}$, причем $\left(\frac{k}{d}, \frac{m}{d}\right) = 1$.
На основанiи предыдущаго, это сравненiе разрѣшимо и имѣет 1 корень mod. $\frac{m}{d}$; ему соотвѣтствуют d корней mod m; если x есть корень послѣдняго сравненiя, причем, для опредѣленности, $0 \leqq x < \frac{m}{d}$, то первоначальное сравненiе имѣет d раз-
? личных корней (mod m): $x, x+\frac{m}{d}, x+\frac{2m}{d}, \ldots x+(d-1)\frac{m}{d}$.
Крайнiй случай: $m \mid k$, т. е. $d=m$. На основанiи предыдущаго, если $m \mid l$, имѣем m различных рѣш. (mod m), т. е. всѣ цѣлыя числа; если же $m \nmid l$, ни одного рѣшенiя.

Резюмируем: сравненiе $kx+l\equiv 0 \pmod m$, гдѣ $(k, m)=d$ имѣет d различных рѣшенiй (mod m) или ни одного, смотря по тому, дѣлит d l или нѣт.

Практически сравненiя можно разрѣшать таким образом. Пусть данное сравненiе есть $kx+l\equiv 0 \pmod m$, гдѣ $(k, m)=1$. [если k и m не взаимно простыя, мы можем привести сравненiе к этому виду, раздѣлив обѣ части на общ. наиб. дел. k и m].
~~Замѣнив x через $-ly$, получим: $kx - kly \equiv l \pmod m$ или $ky \equiv 1 \pmod m$.~~
Разсмотрим сравненiе: $ky \equiv 1 \pmod m$; умножив обѣ части на $-l$, получим: $-kly \equiv -l \pmod m$ или, положив $x=-ly$, $kx \equiv -l \pmod m$, т. е. получим данное сравненiе.

Итак, задача свелась к рѣшенію сравненія

$$ky \equiv 1 \pmod{m}, \text{ причем } (k, m) = 1.$$

Это сравненіе эквивалентно діофантовскому уравненію

$$ky = 1 + mz.$$

1-ый способ.
Для нахожденія y достаточно испытать числа $1, 2, \ldots m-1$; при помощи конечнаго ряда операцій найдем искомый корень.

2-ой способ. Производим над m и k тот же ряд операцій, как при нахожденіи общаго наиб. дѣлителя:

$$m = q_1 k + r_2\ ;\ k = q_2 r_2 + r_3; \ldots; r_{n-2} = q_{n-1} r_{n-1} + 1. \quad [\text{т.к. } (m, k) = 1.].$$

В этих операціях полагаем k положительным; если бы k было отрицательным, мы замѣнили бы его через $k + u m$, гдѣ u достаточно большое цѣл. пол. число, чтобы сумма $k+um$ была положительна.
Из послѣдняго равенства имѣем: $1 = r_{n-2} - q_{n-1} r_{n-1} = r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2} r_{n-2}) = -q_{n-1} r_{n-3} + (1 + q_{n-1} q_{n-2}) r_{n-2}$; из пред. опредѣляем r_{n-2} через r_{n-3} и r_{n-4} и вставляем в это же равенство и т. д. В правой части всегда будет линейная функція от r_i и r_{i+1}. В результатѣ получим:

$$1 = ky + m(-z)$$

Итак, рѣшеніе найдено и попутно дано новое доказательство существованія этого рѣшенія

Примѣр: $31x \equiv 1 \pmod{55}$. Имѣем: $55 = 1.31 + 24$; $31 = 1.24 + 7$; $24 = 3.7 + 3$; $7 = 2.3 + 1$.
Далѣе: $1 = 7 - 2.3 = 7 - 2(24 - 3.7) = 7.7 - 2.24 = 7(31 - 1.24) - 2.24 = 7.31 - 9.24 =$

$=7\cdot31-9(55-1\cdot31)=16\cdot31-9\cdot55$. Итак, $x=16$. Общее решение.

$x=16 \pmod{55}$ или $x=16+n\cdot55$.

Системы сравнений первой степени.

Даны 2 сравнения:

$$x\equiv r \pmod{a}, \quad x\equiv s \pmod{b}$$

Найдем условия их совместности. Пусть $(a,b)=d$. Назовем общее наим. кратное a и b m; $m=\frac{ab}{d}$.

1) случай $r\not\equiv s \pmod{d}$. Нет ни одного общего решения. В с. д. [допустим обратное] из 1-го имеем $x=r+ay$, из 2-го $r+ay\equiv s \pmod{b}$, т. е. $r+ay\equiv s \pmod{d}$, т. е. $r\equiv s \pmod{d}$ — против предположения.

2) случай $r\equiv s \pmod{d}$. Тогда существует 1 решение mod m. 1-ое сравнение равносильно равенству: $x=r+ay$; из 2-го имеем: $r+ay\equiv s \pmod{b}$ или $ay\equiv s-r \pmod{b}$; сравнение разрешимо и имеет d корней (mod b) или 1 корень (mod $\frac{b}{d}$). Если y_0 есть одно из чисел, удовлетворяющих посл. сравнению, то все остальные будут даны формулой:

$$y=y_0+\frac{b}{d}z, \text{ откуда } x=r+ay_0+\frac{ab}{d}z=x_0+mz.$$

Теорема доказана.

Пример: $x\equiv3 \pmod{7}$, $x\equiv5 \pmod{6}$; $x=3+7y$; $3+7y\equiv5 \pmod{6}$ или $7y\equiv2 \pmod{6}$. $y_0=2$, $y=2+6z$; $x=3+14+42z=17+42z$; $x\equiv17 \pmod{42}$.

Переходим к общему случаю; пусть

$$x\equiv r_1 \pmod{a_1}, \dots \; x_z\equiv r_z \pmod{a_z}.$$

Пусть всѣ модули попарно взаимно простые, $(a_u, a_v)=1$,
Докажем, что эта система всегда имѣет одно рѣшеніе $(\mathrm{mod}\ a_1 \dots a_r)$.
В самом дѣлѣ, 2 первых имѣют общее рѣшеніе $x \equiv x_0 \pmod{a_1 a_2}$.
Сопоставляя с этим 3 сравненіе и замѣчая, что модули вз. простые, получим общее рѣшеніе трех сравненій: $x \equiv x_1' \pmod{a_1 a_2 a_3}$ и т. д.

<u>1-ый способ.</u> Назовем $a_1 a_2 \dots a_r = m$. Найдем число b_1 такое, что $b_1 \equiv 1 \pmod{a_1}$ и $b_1 \equiv 0 \pmod{\frac{m}{a_1}}$. Это возможно, т. к. $\left(a_1, \frac{m}{a_1}\right) = 1$.
Затѣм найдем b_2 так, что $b_2 \equiv 1 \pmod{a_2}$, $b_2 \equiv 0 \pmod{\frac{m}{a_2}}$ и т. д.
$b_r \equiv 1 \pmod{a_r}$, $b_r \equiv 0 \pmod{\frac{m}{a_r}}$. Тогда число $b_1 r_1 + b_2 r_2 + \dots + b_r r_r$ удовлетворяет систем. Докажем это. Умножаем 1-ое сравненіе на b_1, 2-ое на b_2, ... r-ое на b_r; получим: $b_1 x \equiv r_1 b_1 \pmod{a_1|b_1|}$ и т. д., $b_r x \equiv r_r b_r \pmod{a_r|b_r|}$. Складываем, замѣчая, что $a_i|b_i| \equiv 0 \pmod m$, и замѣняя модули в правых частях их дѣлителем m, получим:

$$x(b_1+b_2+\dots+b_r) \equiv r_1 b_1 + r_2 b_2 + \dots + r_r b_r \pmod m$$

По извѣстной теоремѣ $b_1+b_2+\dots+b_r \equiv 1 \pmod m$ [$b_k \equiv 1 \pmod{a_k}$, $b_i \equiv 0 \pmod{a_k}$, гдѣ $i \neq k$, сл. $b_1+b_2+\dots+b_r \equiv 1 \pmod{a_k}$, $k=1,2,\dots r$.]
Отсюда слѣдует, что $x \equiv r_1 b_1 + r_2 b_2 + \dots + r_r b_r \pmod m$.

Пусть дано одно сравненіе

$$kx+l \equiv 0 \pmod m, \quad \text{гдѣ } m = p_1^{\alpha_1} \dots p_\rho^{\alpha_\rho}, \quad \text{и } (k, m)=1$$

Это сравненіе равносильно системѣ сравненій

$$kx+l \equiv 0 \pmod{p_1^{\alpha_1}}, \ \dots\ , \ kx+l \equiv 0 \pmod{p_\rho^{\alpha_\rho}}$$

Каждое из сравнений системы даст рѣшеніе (и притом одно)

$x_1 \equiv r_1 \pmod{p_1^{\alpha_1}}, \ldots \quad x \equiv r_\rho \pmod{p_\rho^{\alpha_\rho}}$.

По предыдущему найдем общее рѣшеніе этой системы, которое и будет рѣшеніем (единственным) данного сравненія.

Теорема. Даны 2 положительных цѣлых числа a и b, причем $(a, b) = 1$. Докажем, что $ax + by$ пробѣгает полную систему вычетов mod ab, если x и y пробѣгают соотвѣтственно полную систему вычетов mod b и mod a.

Доказ. Т. к. x получает b различных значеній, y a значеній, то выраженіе $ax+by$ получает ab значеній. Остается доказать, что любые 2 из них не сравнимы по модулю ab.

Допустим, что $ax_1 + by_1 \equiv ax_2 + by_2 \pmod{ab}$.

Отсюда слѣдует, что $ax_1 + by_1 \equiv ax_2 + by_2 \pmod{a}$, т. е.

$by_1 \equiv by_2 \pmod{a}$, или $y_1 \equiv y_2 \pmod{a}$, что ~~невозможно~~

С помощью этой теоремы можно еще раз вывести ~~извѣстное~~ свойство функціи φ, а именно: $\varphi(ab) = \varphi(a) \cdot \varphi(b)$, если $(a, b) = 1$.

Замѣтим, что $\varphi(n)$ представляет также число чисел взаимно простых с n в полной системѣ вычетов $(\bmod\ n)$

Пусть (в пред. теореме) $(x, b) > 1$, тогда $(ax+by, ab) \geq 1$; если $(y, a) > 1$, то тоже $(ax+by, ab) > 1$. Итак, в полной системѣ вычетов mod ab, выражаемых формулой $ax+by$, только тѣ могут быть ~~будут~~ взаимно простых с ab, для кот. $(x, b) = 1$ и $(y, a) = 1$.*) Очевидно, x может принимать $\varphi(b)$ различных значений, а y $\varphi(a)$ разл. значений. Комбинации этих значений для выражения $ax+by$ дадут $\varphi(a)\cdot\varphi(b)$ значений вычетов (mod ab), взаимно простых с ab, т. е. $\varphi(ab) = \varphi(a)\cdot\varphi(b)$.

На основании теории сравнений мы можем решать ур-ия 1ой степени с 2мя неизвестными. Пусть дано такое уравнение

$$ax + by = c. \qquad (1)$$

По пред., $d = (a, b)$ должен делить c; если это условие выполнено, то имеем: $\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$ или $\frac{a}{d}x \equiv \frac{c}{d} \pmod{\frac{b}{d}}$.

Решение посл. ср. будет $x = x_0 + \lambda\frac{b}{d}$; тогда $y = y_0 - \lambda\frac{a}{d}$. ([illegible])

Т. образом мы нашли общее выражение всех (наш) решений неопределенного уравнения 1ой ст. с 2мя неизвестными.

<u>Теорема Fermat</u>. Дано: a целое число, p — простое число; $p \nmid a$.

<u>Тр. док.</u> $a^{p-1} \equiv 1 \pmod p$. Доказательство. Числа $0, 1, 2, \dots p-1$ образуют полную систему вычетов по модулю p; умножив все их на a, получим: $0, a, 2a, \dots, (p-1)a$ — тоже полная система вы-

*) Докажем, что это условие достаточно; пусть $(x, b) = 1$; $(y, a) = 1$.

Тр. док. $(ax+by, ab) = 1$. Допустим обратное: простое число $p \mid ax+by$, $p \mid ab$; пусть $p \nmid b$, тогда $p \mid a$; $p \mid by$, след. $p \mid y$, что противоречит условию $(a, y) = 1$

четов по модулю p. Отсюда следует, что

$$1.2\ldots(p-1) \equiv 1.a.\,2a\ldots(p-1)a \pmod p \quad \text{или}$$

$$(p-1)! \equiv a^{p-1}(p-1)! \bmod(p), \quad \text{т. е.}$$

$$a^{p-1} = 1 \pmod p \qquad \text{что и тр. док.}$$

Эйлерово обобщение теоремы Fermat:

Пусть a и m любые целые числа, ~~m~~ a положительны, и $(a, m) = 1$

Тр. док. $\quad a^{\varphi(m)} \equiv 1 \pmod m.$

Последовательные числа $0, 1, 2, \ldots m-1$ образуют полную систему вычетов (mod m); умножим все члена этой последов. на a,

$$0,\ a,\ 2a, \ldots (m-1)a$$

тоже образуют полную систему вычетов по модулю m.

Из 1-ой последовательности выпишем числа, взаимно простые с m; пусть это будут:

$$b_1, b_2, \ldots b_{\varphi(m)}.$$

Соответственные числа 2-ой системы

$$ab_1, ab_2, \ldots ab_{\varphi(m)}$$

очевидно тоже все будут взаимно простые с m; каждый из членов 1-го ряда сравним с одним из членов 2-го ряда по модулю m. перемножая эти сравнения, найдем:

$$b_1 b_2 \ldots b_{\varphi(m)} \equiv a^{\varphi(m)} \cdot b_1 b_2 \ldots b_{\varphi(m)} \pmod m \quad \text{или, деля на } b_1 b_2 \ldots b_{\varphi(m)}$$

$$a^{\varphi(m)} \equiv 1 \pmod m \qquad \text{что и тр. док.}$$

$2^{ое}$ доказ. теоремы Fermat (Euler). Пусть a любое целое число, p – любое простое число

~~[Пусть $p \nmid a$; пер. док. $a^{p-1} \equiv 1 \pmod p$]~~ [втор. док. тогда $a^p \equiv a \pmod p$].

Исходим из тождества:

$$(u+v)^p = u^p + pu^{p-1}v + \frac{p(p-1)}{1\cdot 2}u^{p-2}v^2 + \dots + \binom{p}{\lambda}u^{p-\lambda}v^\lambda + \dots + v^p,$$

где $\binom{p}{\lambda} = \frac{p(p-1)\dots(p-\lambda+1)}{\lambda!}$

Если p простое число, то все коэф., кроме $1^{го}$ и последнего, делятся на p, т.к. при $1 \leq \lambda \leq p-1$ $\binom{p}{\lambda} = p\frac{(p-1)(p-2)\dots(p-\lambda+1)}{\lambda!}$

Доказываем методом полной индукции. Пусть p – данное простое число. Теорема очевидно справедлива для $a = 1$. Допустим, что теорема справедлива для некоторого a; имеем:

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \dots + 1 \equiv a^p + 1 \pmod p \text{ или}$$

$$(a+1)^p - (a+1) \equiv a^p - a \pmod p \text{ (по осн. предп.) } \equiv 0 \pmod p.$$

Итак, теорема справедлива для всякого a. Заметим, что если $p \nmid a$, обе части сравнения $a^p \equiv a \pmod p$ можно разделить на a; получим теорему Fermat в начальной формулировке; теорема же Эйлера справедливо и для $p \mid a$.

$3^{ье}$ доказательство (Gauss).

Применяя свойство биномиальных коэффициентов к трехчлену и вообще многочлену, мы получим: $(u_1+u_2+u_3)^p \equiv u_1^p+u_2^p+u_3^p \pmod p$ и т.д. Вообще $(u_1+u_2+\dots u_n)^p \equiv u_1^p+u_2^p+\dots u_n^p \pmod p$ (u – числа целые).

Гаусс полагает: $n = a$; $u_1 = u_2 = \dots = u_n = 1$. Получаем:

$$a^p \equiv a \pmod p \quad \text{, что и тр. док.}$$

$2^{ое}$ доказательство обобщенной теоремы.

Лемма. Дано $x \equiv y \pmod{p^\lambda}$, где $\lambda \geq 1$; $\mu \geq 0$ — целое число; тр. док. $x^{(p^\mu)} \equiv y^{p^\mu} \pmod{p^{\lambda+\mu}}$. Доказ. $x = y + p^\lambda z$;

$x^p = (y + p^\lambda z)^p = y^p + p^{\lambda+1} y^{p-1} z + p^{2\lambda} u$ или $x^p \equiv y^p \pmod{p^{\lambda+1}}$;

далее $x^{p^2} \equiv y^{p^2} \pmod{p^{\lambda+2}}$ и т. д. Наконец, $x^{p^\mu} \equiv y^{p^\mu} \pmod{p^{\lambda+\mu}}$.

Теорема. Дано $(a, m) = 1$, тр. док. $a^{\varphi(m)} \equiv 1 \pmod m$.

Доказ. Пусть $m = p_1^{\mu_1} p_2^{\mu_2} \ldots p_s^{\mu_s}$. Ни одно из чисел p не делит a, след. $a^{p-1} \equiv 1 \pmod p$. (возводим в ст. $p^{\mu-1}$) На основании леммы $a^{p^{\mu-1}(p-1)} \equiv 1 \pmod{p^\mu}$

Итак $a^{\varphi(p^\mu)} \equiv 1 \pmod{p^\mu}$; но $\varphi(m) = \varphi(p_1^{\mu_1}) \cdot \varphi(p_2^{\mu_2}) \ldots \varphi(p_s^{\mu_s})$.

$\varphi(p^\mu) \mid \varphi(m)$; a fortiori мы имеем:

$$a^{\varphi(m)} \equiv 1 \pmod{p_1^{\mu_1}};\ a^{\varphi(m)} \equiv 1 \pmod{p_2^{\mu_2}}; \ldots\ a^{\varphi(m)} \equiv 1 \pmod{p_s^{\mu_s}}.$$

По одной из предыдущих теорем отсюда следует:

$$a^{\varphi(m)} \equiv 1 \pmod m. \qquad \text{Что и тр. док.}$$

Следствия теоремы Fermat:

1) Дано сравнение $x^2 \equiv -1 \pmod p$; тр. доказать, что или $p = 2$ или $p \equiv 1 \pmod 4$. Доказ. Пусть $p \equiv 3 \pmod 4$, т. е. $p = 4u + 3$. По теореме Ферма $x^{p-1} \equiv 1 \pmod p$; у нас $p - 1 = 4u + 2 = 2(2u+1)$, т. е. $\frac{p-1}{2}$ нечетное число; обе части данного сравнения возводим в степень $\frac{p-1}{2}$; находим:

$x^{p-1} \equiv -1 \pmod p$ или $1 \equiv -1 \pmod p$ или $2 \equiv 0 \pmod p$, что невозможно

2) Мы видели что при $(a, m) = 1$ $a^{\varphi(m)} \equiv 1 \pmod{m}$, т. е. при данных a и m всегда найдется такое число μ, что $a^{\mu} \equiv 1 \pmod{m}$. ~~Среди этих есть наименьшее~~; пусть $a^{\mu} \equiv a^{\nu} \pmod{m}$, где $1 \leq \mu < \nu$
$a^{\mu} \equiv a^{\mu} \cdot a^{\nu-\mu} \pmod{m}$ или $a^{\nu-\mu} \equiv 1 \pmod{m}$; ~~пусть $\nu-\mu$~~. Если λ есть наименьшее из чисел для кот. $a^{\lambda} \equiv 1 \pmod{m}$, то λ называется показателем, к которому принадлежит $a \pmod{m}$.

Теорема. Дано $a^{x} \equiv 1 \pmod{m}$; тр. док. $\lambda | x$. Доказ. $x = q\lambda + r$; допустим что $r \neq 0$. Имеем: $1 \equiv a^{x} = a^{q\lambda} \cdot a^{r} \equiv a^{r} \pmod{m}$, т. е. $a^{r} \equiv 1 \pmod{m}$, т. к. λ не есть наименьшее число, что противоречит предположению.

Теорема. В ряде $a, a^2, \ldots a^{\lambda-1}, a^{\lambda}$ нету двух чисел, сравнимых между собою $\pmod{m}$. Допустим, что $a^{\mu} \equiv a^{\nu} \pmod{m}$; $1 \leq \mu < \nu \leq \lambda$;
Имеем $1 \equiv a^{\nu-\mu}$, т. е. λ не было бы наименьшим; Если μ и ν любые числа, то последняя формула показывает, что $a^{\mu} \equiv a^{\nu} \pmod{m}$ только в том случае, если $\mu \equiv \nu \pmod{\lambda}$.
Заметим, на осн. предыдущего, что $\lambda \leq \varphi(m)$ и $\lambda | \varphi(m)$.

О числе корней сравнений.

Рассмотрим некоторые примеры. Сравнение $2x \equiv 0 \pmod{6}$ имеет 2 корня $x \equiv 0$ и $x \equiv 3 \pmod{6}$. Сравнение $x^2 \equiv 1 \pmod{8}$ имеет 4 корня: $x \equiv 1, 3, 5, 7 \pmod{8}$; сравнение $x^2 \equiv 2 \pmod{3}$ не имеет ни одного корня.

Докажем общую теорему; пусть дано сравнение

$f(x)=c_0x^n+c_1x^{n-1}+\ldots+c_n\equiv 0 \pmod p$, где p простое, $n\geq 1$, $p\nmid c_0$,

требуется доказать, что число корней этого сравнения $\leqq n$.

(Заметим, что c_0 можно всегда предполагать $=1$; в самом деле, положим $c_0t\equiv 1 \pmod p$; отсюда можно всегда найти t. Умножаем данное сравнение на t; имеем:

$tc_0x^n+tc_1x^{n-1}+\ldots+tc_n\equiv 0 \pmod p$ или $x^n+b_1x^{n-1}+\ldots+b_n\equiv 0 \pmod p$;

где все b опять целые числа).

Докажем теорему методом полной индукции; мы знаем, что она справедлива для $n=1$. Пусть ξ какое-нибудь целое число. Тогда

$$\frac{f(x)-f(\xi)}{x-\xi}=\frac{c_0(x^n-\xi^n)+c_1(x^{n-1}-\xi^{n-1})+\ldots+c_{n-1}(x-\xi)}{x-\xi}=c_0(x^{n-1}+x^{n-2}\xi+\ldots+\xi^{n-1})+c_1(x^{n-2}+\ldots)+\ldots+c_{n-1}=$$

$$=c_0x^{n-1}+b_1x^{n-2}+\ldots+b_{n-2}x+c_{n-1}=g(x),\ \text{т. е.}$$

$$f(x)-f(\xi)=(x-\xi)g(x) \qquad (1)$$

Допустим, что теорема справедлива для сравнений $n-1$-ой ст. и убедимся, что она верна для сравнений n-ой ст. Пусть сравнение $f(x)$ имеет более n, напр. $n+1$ корней, несравнимых $(\mathrm{mod}\ p)$, именно $\xi, \xi_1, \xi_2, \ldots \xi_n$. Подставляя в формулу (1) на место x ξ_1, имеем: $f(\xi_1)-f(\xi)=(\xi_1-\xi)g(\xi_1)$ или $0\equiv(\xi_1-\xi)g(\xi_1)$.

Т. обр. ξ_1 есть корень сравнения $g(x)\equiv 0 \pmod p$ степени $n-1$; совершенно также убедимся, что $\xi_2, \xi_3, \ldots \xi_n$ суть корни сравнения $g(x)\equiv 0$, т. е.

сравнение $n-1^{\text{ой}}$ ст. имеет n корней, что противно допущению. Теорема доказана.

Отсюда следует, что, если сравнение $c_0x^n+c_1x^{n-1}+\dots+c_n\equiv 0 \pmod p$ имеет более n разных корней, то имеем: $p|c_0$, $p|c_1$, … $p|c_n$, и сравнению удовлетворяет любое целое число.

Пусть $a_0x^n+a_1x^{n-1}+\dots+a_n\equiv b_0x^n+b_1x^{n-1}+\dots+b_n \pmod p$ имеет большее, чем n, корней; тогда $a_0\equiv b_0$, $a_1\equiv b_1$, … $a_n\equiv b_n \pmod p$.

Пусть теперь дано сравнение:

$$x^n+a_1x^{n-1}+\dots+a_n\equiv x^n+b_1x^{n-1}+\dots+b_n \pmod p;$$

то оно равносильно сравнению $n-1^{\text{ой}}$ степени; если обе функции сравнимы между собою более, чем для $n-1$ значений x, то

$$a_1\equiv b_1, \dots\ a_n\equiv b_n \pmod p.$$

Применим это к сравнению

$$x^{p-1}-1\equiv(x-1)(x-2)\dots(x-(p-1)) \pmod p.$$

Это сравнение имеет корни $1, 2, \dots (p-1)$, числом больше, чем $p-2$; на основании предыдущего, коэффициенты при одинаковых степенях x и постоянные обеих частей сравнимы между собою $\pmod p$. ~~Наконец~~ Итак

$$-1\equiv(-1)^{p-1}(p-1)! \pmod p$$ [формула верна и для $p=2$]

или для $p>2$ $\quad (p-1)!\equiv -1 \pmod p$. Это т. наз. формула Wilson'a.

Свойство, выражаемое формулой Вильсона, характеристично

для простых чисел, т.к. для числа составного m очевидно
$(m-1!, m)>1$
~~$(m-1)! \equiv 0 \pmod{m}$~~. [отсюда следует $\frac{(p-1)!+1}{p}$ есть целое число].

2-ой способ доказательства (Gauss).

Рассмотрим ряд чисел: $1, 2, \ldots, p-1$. Пусть одно из них есть r. Сравнение $rs \equiv 1 \pmod{p}$ даст для s число того же ряда. Могут быть 2 случая: 1) $s=r$, 2) $s \neq r$. Для 1-го случая имеем:

$r^2 \equiv 1 \pmod{p}$ или $(r-1)(r+1) \equiv 0$; т.е. из нашего ряда это будут только числа 1 и $p-1$; все остальные разбиваются на пары. Произведение

$$(p-1)! \equiv 1 \cdot (-1) \equiv -1 \pmod{p} \quad \text{что и тр. док.}$$

Пусть $0 < a < p-1$; $(p-1)! = 1.2\ldots(p-1-a).(p-a)\ldots(p-1) \equiv (p-1-a)!(-a)(-a+1)\ldots(-1) \equiv$
$\equiv (-1)^a a!(p-1-a)!$, т.е. $a!(p-1-a)! \equiv (-1)^{a+1} \pmod{p}$.

Полагаем $a=1$. Имеем: $(p-2)! \equiv 1 \pmod{p}$. Пусть $p>2$, т.е. нечетное; полагаем $a=\frac{p-1}{2}$. Прилагая формулу, имеем

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \begin{cases} \equiv +1, & \text{если } p \equiv 3 \pmod{4} \\ \equiv -1, & \text{если } p \equiv 1 \pmod{4} \end{cases}$$

Исследуем сравнение $x^2 \equiv -1 \pmod{p}$: оно очевидно разрешимо при $p=2$. Для $p>2$ оно разрешимо, если $p \equiv 1 \pmod{4}$ и неразрешимо, если $p \equiv 3 \pmod{4}$. ~~Докажем, что~~ В самом деле, возводим сравнение в степень $\frac{p-1}{2}$; в 1-ом случае имеем $x^{p-1} \equiv 1 \pmod{p}$; во 2-ом $x^{p-1} \equiv -1 \pmod{p}$, что противор. теореме Fermat.

Докажем <u>теорему</u>: существует бесчисленное множество простых чисел типа $p \equiv 1 \pmod 4$. Допустим, что их число конечно: $5, 13, 17, \ldots p$. Составим выражение

$$2^2 \cdot 5^2 \cdot 13^2 \ldots p^2 + 1.$$

Это число нечетное, не делящееся на $5, 13, \ldots p$. ~~Если бы все его~~ простые. Если бы его делитель простой q имел форму $q \equiv -1 \pmod 4$, то сравнение ~~множители были типа $q \equiv 1 \pmod 4$, то оно было бы~~ $x^2+1 \equiv 0 \pmod q$ имело бы корень ~~простое~~ $x = 2\cdot 5 \cdot 13 \ldots p$, что противоречит пред. теореме ~~вида $4Q-1$; значит, есть (число $q > p$, $q \equiv 1 \pmod 4$)~~

<u>Теорема</u>. Дано: $f(x) = \varphi(x)\psi(x)$, где f, φ и ψ суть целые целочисленные многочлены степеней n, m, l; Тр. док. если $\varphi(x) \equiv 0 \pmod p$ имеет m корней; $\psi(x) \equiv 0 \pmod p$ им. l корней, ~~Тр. док.~~ $f(x) \equiv 0 \pmod p$ имеет $n = m + l$ корней; обозначим число корней f через (f). Ясно, что $(f) \leqq (\varphi) + (\psi)$; $(\varphi) \leqq m$, $(\psi) \leqq l$; $(\varphi) + (\psi) \leqq m + l$. С другой стороны $(\varphi) + (\psi) \geqq (f) = m + l$, $(f) = (\varphi) + (\psi)$, т. е. $(\varphi) = m$, $(\psi) = l$ *)

Пример. Мы видели, что сравнение

$$x^{p-1} - 1 \equiv 0 \pmod p$$

имеет как раз $p-1$ различных корней (т. е. максимальное число); если $p > 2$, то p нечетно, и мы можем разложить левую часть на 2 множителя $\left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p$. По предыдущему каждое из сравнений $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$ и $x^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$ имеет по $\frac{p-1}{2}$ разных корней

---

*)

Мы видели, что если k есть наименьшее из чисел, для кот. $x^k\equiv 1 \pmod p$, то $k \mid p-1$, и мы называли x числом, принадлежащим к показателю k по модулю p.

Обратная теорема состоит в следующем: если дано $k \mid p-1$, то существует число x, удовлетворяющее сравнению $x^k\equiv 1 \pmod p$, причем для этого x не удовлетворяется сравнение того же вида с показателем $k'<k$. Эту теорему мы докажем после ряда последующих рассуждений.

Замечание: если $n \mid p-1$, то $x^n-1 \mid x^{p-1}-1$; в самом деле, положим $x^n=y$, $x^{p-1}=y^b$, имеем $\frac{x^{p-1}-1}{x^n-1}=\frac{y^b-1}{y-1}=y^{b-1}+y^{b-2}+\dots+y+1=x^{p-1-n}+x^{p-1-2n}+\dots+x^n+1=$ целое число.

Лемма. Дано: $x^r\equiv 1 \pmod p$; $x^s\equiv 1\pmod p$; $(r,s)=t$. Тр. док. $x^t\equiv 1 \pmod p$. Доказ. Мы можем всегда разрешить неопр. уравнение $t=ru-sv$ или $1=\frac{r}{t}u-\frac{s}{t}v$; при этом можно найти для u и v пару положительных значений. Имеем: $ru=t+sv$, отсюда $x^{ru}\equiv x^t\cdot x^{sv}\equiv x^t \pmod p$. Сл. $x^t\equiv 1 \pmod p$, что и тр. док.

Пусть теперь v - любое положит. число. На основании доказанной леммы сравнения $x^v\equiv 1 \pmod p$ и $x^{p-1}\equiv 1 \pmod p$ имеют общими все корни сравнения $x^{(v,p-1)}\equiv 1 \pmod p$.

Пусть $n \mid p-1$. По только что доказанному все корни сравнения $x^n\equiv 1 \pmod p$ суть корни сравнения $x^{p-1}\equiv 1 \pmod p$. Если x, корень сравнения $x^n\equiv 1 \pmod p$, не удовлетворяет никакому сравнению того же вида, но низшей степени, что он не д. первообразным корнем этого сравнения. Значит, всякий непервообразный корень этого сравнения удовлетворяет сравнению $x^u \equiv 1 \pmod p$, где $u < n$. Очевидно, что наименьшее $u \mid n$.

Число корней сравнения $x^n \equiv 1 \pmod p$ есть n, т.к. $x^n - 1 \equiv 0$ ~~(mod p)~~ есть множитель $x^{p-1}-1$, кот. в сравнении $\equiv 0 \pmod p$ имеет максимальное число корней. Из этих n корней некоторое количество может быть непервообразными; число первообразных же будет $\psi(n)$ (~~[illegible]~~), некоторая функция числа n. Изучим свойства этой функции. Очевидно, все n корней сравнения $x^n \equiv 1 \pmod p$ суть первообразные корни или этого самого сравнения или сравнения $x^d \equiv 1 \pmod p$, где $d \mid n$. Итак, получаем тождество:

$$n = \sum_{d \mid n} \psi(d).$$

Пусть $\delta \mid n$; на основ. предыдущего равенства $\frac{n}{\delta} = \sum_{d \mid \frac{n}{\delta}} \psi(d)$. Умножаем обе части на $\mu(\delta)$ и суммируем по δ. В левой части получится известное выражение функции $\varphi(n)$. Итак, имеем:

$$\varphi(n) = \sum_{\delta \mid n} \mu(\delta)\frac{n}{\delta} = \sum_{\delta \mid n} \sum_{d \mid \frac{n}{\delta}} \psi(d)\mu(\delta) = \sum_{\substack{d\delta \mid n \\ \delta, d}} \psi(d)\mu(\delta) =$$

$$= \sum_{d \mid n} \psi(d) \sum_{\delta \mid \frac{n}{d}} \mu(\delta) = \psi(n). \quad \text{Итак } \varphi(n) \equiv \psi(n).$$

Итак, число первообразных корней сравнения $x^n \equiv 1 \pmod p$, где $n \mid p-1$, равно числу чисел, меньших n и с ним взаимно простых. Одновременно этим самым мы доказали существование чисел, принадлежащих к показателю n по модулю p.

Первообразные корни сравнения $x^{p-1} \equiv 1 \pmod p$ называются просто первообразными корнями (по Hilbert'у — первообразными числами) по модулю p; их число, конечно — $\varphi(p-1)$.

Эти корни образуют циклическую группу. Пусть g некоторый один из этих корней. Тогда все числа ряда

$$g^0, g^1, g^2, \dots g^{p-2}$$

между собой не сравнимы $\pmod p$. В.с.д., допустим обратное, пусть $g^\lambda \equiv g^\mu \pmod p$ $(p-2 \geq \lambda > \mu)$ или $g^{\lambda-\mu} \equiv 1 \pmod p$; т.к. $\lambda - \mu < p-1$, то g не было бы первообразным корнем $\pmod p$, что противно предпол.

Написанные степени g эти суть представители всех классов чисел по модулю p взаимно простых с p; независимо от порядка, этот ряд сравним $\pmod p$ с $1, 2, \dots p-1$.

Предыдущее замечание можно обобщить: система чисел g^ν, где ν принимает все значения какой-нибудь полной системы вычетов $\bmod (p-1)$, является представителями всех классов чисел $\pmod p$ взаимно-простых с p. Из этих чисел тѣ, для которых $(\nu, p-1) = 1$, будут первообразными корнями. В самом дѣлѣ, очевидно $g^{\nu(p-1)} \equiv 1 \pmod p$; пусть $g^{\nu y} \equiv 1 \pmod p$. Тогда $p-1 \mid \nu y$, значит $p-1 \mid y$; $y \geq p-1$; g^ν дѣйствительно первообразный корень.

Если же $(\nu, p-1) > 1$, то g^{ν} не первообразный корень. Пусть $y = \frac{p-1}{(\nu, p-1)} < p-1$; $g^{\nu y} = g^{\frac{\nu(p-1)}{(\nu,p-1)}} = g^{M} \equiv 1$, где M - наим. кратное ν, $p-1$. Итак g^{ν}, в степени меньшей $p-1$, $\equiv 1 \pmod{p}$, т. е. g^{ν} не первообр. корень.

Из предыдущего следует, что если известен один первообразный корень $\pmod{p}$, то все другие найдутся помощью арифметических действий; для нахождения же 1-го приходится испытывать числа, взаимно простые с p, н. с. $2, 3, \ldots p-1, p+1, \ldots$

Глава 6. О квадратичных вычетах.

Общий вид сравнения 2-ой степени таков:

$$ax^2+bx+c \equiv 0 \pmod{m} \quad (1)$$ причем $a \not\equiv 0 \pmod{m}$.

Приведем левую часть к нормальному виду; умножаем обе части и модуль на $4a$; новое сравнение будет эквивал. данному

$$4a(ax^2+bx+c) \equiv 0 \pmod{4am}$$ или

$$(2ax+b)^2-(b^2-4ac) \equiv 0 \pmod{4am}.$$

Полагаем $b^2-4ac = D$, $4am = k$, $2ax+b = z$. Получим сравнение в нормальном виде $z^2 \equiv D \pmod{k}$ (2). Мы будем искать (значения) значения x, удовлетворяющие (1) сравнению; очевидно для этого надо найти значения z целые и такие, чтобы $\frac{z-b}{2a}$ было целым числом. В последующем мы будем рассматривать только нормальные сравнения

$$x^2 \equiv D \pmod{k}.$$

Если это сравнение разрешимо, то D называется квадратичным вычетом от k или по модулю k, в противном случае D есть квадратичный невычет.

Заметим, что можно всегда предполагать $(D, k) = 1$. В самом деле, пусть в данном сравнении $(D, k) > 1$. Пусть

$$(D, k) = d = \Pi p^{2a} \cdot \Pi p'^{2a'+1} = \left(\Pi p^{a} \Pi p'^{a'}\right)^2 \Pi p' = m^2 q.$$

Очевидно $d \mid x^2$, т.е. $m^2 q \mid x^2$, отсюда $m \mid x$; докажем, что $mq \mid x$.

Мы имеем: $\Pi p^{2a} \Pi p'^{2a'+1} \mid x^2$; отсюда $p^{2a} \mid x^2$, т.е. $p^{a} \mid x$; далее, $p'^{2a'+1} \mid x^2$, след. $p'^{a'+1} \mid x$; т. обр. $\Pi p^{a} \Pi p'^{a'+1} \mid x$, т.е. $mq \mid x$, что и треб. док. или $m \mid x$, $q \mid \frac{x}{m}$. Пусть $D = D_0 \cdot d$, $k = k' \cdot d$. Делаем подстановку

$x = mqy$; получаем:

$$m^2 q^2 y^2 \equiv D_0 m q^2 \pmod{k' m q^2} \quad \text{или}$$

$$q y^2 \equiv D_0 \pmod{k'}.$$

Разберем 2 случая: 1) $(q, k') > 1$. Сравнение в этом случае неразрешимо, т. к. общий делитель чисел q и k' не делит D_0.

2) $(q, k') = 1$. Тогда существует такое r, что $qr \equiv 1 \pmod{k'}$;

Умножаем обе части сравнения на r; получим

$$q r y^2 \equiv r D_0 \pmod{k'} \quad \text{или} \quad y^2 \equiv D' \pmod{k'},$$ где $D' = D_0$

и $(D', k') = 1$. Т. обр. мы привели сравнение к виду, где $(D, k) = 1$.

Примѣръ: $x^2 \equiv 450 \pmod{525}$; $d = 75 = 3 \cdot 5^2$; $q = 3$, $m = 5$. Подстановка $x = 15y$; $3^2 5^2 y^2 \equiv 6 \cdot 75 \pmod{7 \cdot 75}$ или $3y^2 \equiv 6 \pmod 7$. Находим r по условію $3r \equiv 1 \pmod 7$, $r = 5$; $15y^2 \equiv 30 \pmod 7$ или $y^2 \equiv 2 \pmod 7$. Послѣднее сравненіе может имѣть max. 2 корня; в дан. случаѣ это будут: $y \equiv 3$, $y \equiv -3 \equiv 4 \pmod 7$. Общія выраженія y будут: $y = 3 + 7n$, $y = 4 + 7n$; т. е. $x = 45 + 105n$, $x = 60 + 105n$. Получим всѣ корни mod 525; это будут: 1) $x \equiv 45, 150, 255, 360, 465 \pmod{525}$;

2) $x \equiv 60, 165, 270, 375, 480 \pmod{525}$.

Переходим к 1-ой задачѣ, касающейся сравненій 2-ой степени; будем предполагать к данному: найти всевозможные вычеты (и невычеты) и число корней сравненія по модулю k. Отправляемся от сравненія

$$x^2 \equiv D \pmod k.$$

I случай. $k = 2$; D очевидно нечетное. Наше сравненіе принимает вид $x^2 \equiv 1 \pmod 2$; оно имѣет только 1 корень $x \equiv 1 \pmod 2$. по теор. Ферм.

II. $k = p$, гдѣ p — нечетное простое число. Мы предполагаем $1 \leq D \leq p-1$. Сравненіе принимает вид $x^2 \equiv D \pmod p$. Если это сравненіе имѣет 1 корень x, то оно имѣет и другой корень $-x$; в. с. д. $(-x)^2 = x^2 \equiv D \pmod p$. Кромѣ того, $x \not\equiv -x$; иначе мы имѣли бы $2x \equiv 0 \pmod p$ или $x \equiv 0 \pmod p$ — абсурд. Для различных значеній D получится $p-1$ разных сравненій: посмотрим, какія из них разрѣшимы, какія нѣт, иначе говоря, раздѣлим всѣ значенія D на вычеты и невычеты.

Теорема. Из $p-1$ значений D $\frac{p-1}{2}$ суть вычеты и $\frac{p-1}{2}$ — невычеты.

Предполагая, что наше сравнение разрешимо, возводим обе части его в степень $\frac{p-1}{2}$; замечая, что $(x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1$, имеем:

$$D^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Это сравнение имеет $\frac{p-1}{2}$ различных корней. Теорема доказана.

По Эйлеру, если D есть невычет, то она удовлетворяет сравнению $D^{\frac{p-1}{2}} \equiv -1 \pmod p$, а если вычет, то предыдущему (Эйлеров критерий). т. е. $D^{\frac{p-1}{2}} \equiv 1 \pmod p$

В с. д. сравнению $D^{p-1} \equiv 1 \pmod p$ удовлетворяют все числа $1, 2, \ldots p-1$. Это сравнение равносильно двум:

$$D^{\frac{p-1}{2}} \equiv 1 \pmod p, \quad D^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Первому удовлетворяют, по доказанному, все вычеты, сл. остающиеся $\frac{p-1}{2}$ невычетов удовлетворяют 2-му сравнению, что и тр. док.

В связи с теорией квадратичных вычетов целесообразно ввести символ Legendre'а: $\left(\frac{D}{p}\right)$. Этот символ имеет смысл только для p — простого нечетного числа и для случая $(D, p) = 1$; при этом

$$\left(\frac{D}{p}\right) = \begin{cases} = 1, & \text{если } D \text{ вычет от } p \\ = -1, & \text{если } D \text{ невычет } p. \end{cases}$$

Эйлерову теорему можно коротко формулировать так

$$D^{\frac{p-1}{2}} \equiv \left(\frac{D}{p}\right) \pmod{p}.$$

__Теорема.__ ~~Свойст~~ Дано $D \equiv D' \pmod{p}$. ~~Тр.~~ док. причем $p \nmid D, D'$. $\left(\frac{D}{p}\right) = \left(\frac{D'}{p}\right)$, т.-е. $\left(\frac{D}{p}\right)$ есть периодическая функция D с периодом p. Доказат.: мы имеем $x^2 \equiv D \equiv D' \pmod{p}$. Очевидно, оба сравнения эквивалентны, т.е. D и D' одновременно будут вычетами или невычетами, что и т. д.

Если мы представим полную систему вычетов (mod p), взаимно простых с p, в виде $g^0, g^1, g^2, \dots g^{p-2}$, то половина из них будут квадратичные вычеты от p, другие невычеты. Квадратные числа этой системы очевидно суть вычеты, сл. все остальные числа — невычеты. Итак, получаем полную систему квадратич. вычетов в виде

$$g^0, g^2, g^4, \dots g^{p-3}.$$

Доказательство __Dirichlet__ Эйлерова критерия. т.-е. p нечетное. Т. к. $(D, p) = 1$, то сравнение $rs \equiv D \pmod{p}$ для данного r дает одно s и обратно, причем $1 \leq r \leq p-1$, $1 \leq s \leq p-1$. Рассмотрим 2 случая:

1) D невычет; тогда ни одно r не равно соответствующему s; все числа $1, 2, \dots p-1$ будут разбиты на пары, числом $\frac{p-1}{2}$. Перемножаем все сравнения $rs \equiv D \pmod{p}$ для всех полученных пар r, s:
$D^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \pmod{p}$. (стр. 46)

2) D есть вычет. Тогда из чисел $1, 2, \dots p-1$ найдется 2 таких, r' и r'', что $r'r' \equiv D \pmod{p}$ и $r''r'' \equiv D \pmod{p}$; остальные $p-3$ числа разобьются

на $\frac{p-3}{2}$ пар. Замѣтим, что $r'r''\equiv -r'^2\equiv -D$. Перемножая, как в предыдущем случаѣ, находим: $D^{\frac{p-3}{2}}\cdot(-D)\equiv(p-1)!\equiv -1 \pmod p$, т. е. $D^{\frac{p-1}{2}}\equiv 1 \pmod p$, что и тр. док.

Свойства квадратичных вычетов.

1) $R.R=R$; 2) $R.N=N$; 3) $N.N=R$, гдѣ R обозначает вычет, а N-невычет, или символически, в видѣ одной формулы $\left(\frac{D}{p}\right)\cdot\left(\frac{E}{p}\right)=\left(\frac{DE}{p}\right)$

1) $x^2\equiv D \pmod p$ разрѣшимо, $y^2\equiv E \pmod p$ тоже. Перемножаем сравнения $(xy)^2\equiv DE \pmod p$, т. е. DE вычет.

2) Выписываем ~~полную~~ произвольную систему вычетов $(\mathrm{mod}\ p)$, взаимно простых с p, и распредѣляем их на квадратичные вычеты и невычеты. Получим $R_1, R_2, \dots R_{\frac{p-1}{2}}$

$N_1, N_2 \dots N_{\frac{p-1}{2}}$.

Пусть R - произвольное число, сравнимое $(\mathrm{mod}\ p)$ с одним из чисел 1ой строки. Умножаем на него всю нашу систему: $RR_1, RR_2, \dots RR_{\frac{p-1}{2}}$

$RN_1, RN_2, \dots RN_{\frac{p-1}{2}}$.

Получаем опять $p-1$ несравнимых чисел; из них $\frac{p-1}{2}$ в 1ой строкѣ будут по предыдущему, всѣ квадратичные вычеты; сл. всѣ числа 2ой строки будут невычеты. Итак, от умножения любого вычета на любой невычет получается невычет.

3) Умножаем обѣ строки предыдущей схемы на N, гдѣ N сравнимо с каким-нибудь из вычетов 2ой стр. Получаем: $NR_1, NR_2, \dots NR_{\frac{p-1}{2}}$

$NN_1, NN_2, \dots NN_{\frac{p-1}{2}}$.

По предыдущему, вся 1-ая строчка состоит из невычетов, сл. вся 2-ая из вычетов. Итак, от перемножения любых 2 невычетов получается вычет. Теорема доказана.

Докажем ту же теорему помощью Эйлерова критерія.

1) Дано $D^{\frac{p-1}{2}}\equiv 1$, $E^{\frac{p-1}{2}}\equiv 1$; откуда $(DE)^{\frac{p-1}{2}}\equiv 1$, что и тр. док.

2) Дано $D^{\frac{p-1}{2}}\equiv 1$, $E^{\frac{p-1}{2}}\equiv -1$, откуда $(DE)^{\frac{p-1}{2}}\equiv -1$, что и тр. док.

3) Дано: $D^{\frac{p-1}{2}}\equiv -1$, $E^{\frac{p-1}{2}}\equiv -1$, откуда $(DE)^{\frac{p-1}{2}}\equiv 1$, что и тр. док.

Если $D=E$, то $\left(\frac{D}{p}\right)\cdot\left(\frac{D}{p}\right)=\left(\frac{D^2}{p}\right)=1$, как это видно и непосредственно.

Вообще, $\left(\frac{D_1}{p}\right)\cdot\left(\frac{D_2}{p}\right)\dots\left(\frac{D_r}{p}\right)=\left(\frac{D_1 D_2\dots D_r}{p}\right)$. ~~Левая сторона~~ это выраженіе $=1$, т.е. ~~есть~~ произведеніе $D_1D_2\dots D_r$ есть квадратичный вычет, если в него входит четное число производителей невычетов.

III. Модуль есть степень простого числа $k=p^\lambda$; $\lambda\geq 2$, $p\nmid D$, $p>2$

Сравненіе имеет вид: $x^2\equiv D \pmod{p^\lambda}$.

Очевидно, всякое рѣшеніе этого сравненія удовлетворит сравненію $x^2\equiv D\pmod p$, т.е. необходимое условіе разрѣшимости данного сравненія D должно быть квадратичным вычетом числа p.

Докажем, что это условіе и достаточно. Допустим, что оно справедливо для $\lambda=\nu$. Тр. док., что сравненіе $x^2\equiv D \pmod{p^{\nu+1}}$ тоже разрѣшимо. Делаем подстановку $x=a+p^\nu y$, где a есть корень сравненія $x^2\equiv D\pmod{p^\nu}$. Получаем:

$$a^2+2ap^\nu y+\underbrace{p^{2\nu}y^2}_{\equiv 0}\equiv D \pmod{p^{\nu+1}}$$

(переносим все в одну часть)

Делим обе части и модуль на p^ν; находим

$$\frac{a^2-D}{p^\nu}+2ay\equiv 0 \pmod p$$

$\frac{a^2-D}{p^\nu}$ - целое число, т.к. $a^2\equiv D \pmod{p^\nu}$. Это сравнение разрешимо, если $(2a,p)=1$, что справедливо, т.к. $p>2$. Оно дает нам значение y, а значит и x. Итак, сравнение с модулем $p^{\nu+1}$ разрешимо при тех же условиях, как с модулем p^ν. Теорема справедлива для $\nu=1$, след. для всякого ν. Итак, необходимое и дост. условие разрешимости сравнения $x^2\equiv D \pmod{p^\lambda}$, есть $\left(\frac{D}{p}\right)=1$.

Если a есть корень нашего сравнения, то $-a$ - также; очевидно $a\not\equiv -a \pmod p$. Докажем, что других корней нет. Пусть $a^2\equiv D \pmod{p^\lambda}$ и $b^2\equiv D \pmod{p^\lambda}$. тр. док. $b\equiv \pm a$. Исключаем D из 2х сравнений; имеем:

$$(a+b)(a-b)\equiv 0 \pmod{p^\lambda},\text{ т.е. } b\equiv \pm a \pmod{p^\lambda}, \text{ что и тр. док.}^{*)}$$

Число корней сравнения II и III можно изобразить так: $1+\left(\frac{D}{p}\right)$.

Пример. $x^2\equiv 3 \pmod{121}$; узнаем, разрешимо ли сравнение $x^2\equiv 3 \pmod{11}$; Эйлеров критерий дает: $3^{\frac{11-1}{2}}=3^5=243\equiv 1 \pmod{11}$. Сравнение разрешимо, один из его корней $x\equiv 5$. Полагаем $x=5+11y$; $25+10\cdot 11y\equiv 3 \pmod{121}$; $2+10y\equiv 0 \pmod{11}$ $y=2$, $x\equiv 27 \pmod{121}$.

IV. Пусть $k=2^\lambda$, где $\lambda\geq 2$. Сравнение имеет вид:

$$x^2\equiv D \pmod{2^\lambda} \quad \text{где } (D,2)=1.$$

Мы видели, что при $\lambda=1$ сравнение имело один корень. Если $\lambda=2$, то

*) p может входить фактором лишь в одно из выражений $a+b$ и $a-b$; допустив противное, мы имели бы: $p|a+b$, $p|a-b$, сл. $p|2a$, $p|a$, а это невозможно.

сравнение $x^2\equiv D \pmod 4$ имеет: 2 корня, если $D\equiv 1 \pmod 4$ и ни одного, если $D\equiv 3 \pmod 4$, т. к. квадрат всякого нечетного числа имеет вид $4n+1$.

$\lambda=3$. Сравнение $x^2\equiv D \pmod 8$. Если $D\equiv 1 \pmod 8$, то сравнение имеет 4 корня, т. к. квадраты всех нечетных чисел имеют вид $8n+1$; если же $D\equiv 3, 5, 7 \pmod 8$, то наше сравнение не имеет ни одного корня.

$\lambda>3$. Если $D\not\equiv 1 \pmod 8$, то, по предыдущему, сравнение не имеет ни одного корня. Докажем, что, если $D\equiv 1 \pmod 8$, то сравнение разрешимо и имеет 4 корня. Докажем сначала, что в этом случае сравнение всегда имеет корни. Пусть это справедливо для сравнения $x^2\equiv D \pmod{2^\nu}$, где $\nu\geq 3$; докажем, что сравнение $x^2\equiv D \pmod{2^{\nu+1}}$ разрешимо. Если a корень 1-го из написанных сравнений, то $\frac{a^2-D}{2^\nu}$ — целое число. Делаем подстановку: $x=a+2^{\nu-1}y$; получаем:

$$a^2+2^\nu ay+2^{2\nu-2}y^2-D\equiv 0 \pmod{2^{\nu+1}}$$ или, деля на 2^ν

$$\frac{a^2-D}{2^\nu}+ay\equiv 0 \pmod 2.$$ Это сравнение разрешимо, значит и ср. $x^2\equiv D \pmod{2^{\nu+1}}$.

Итак, сравнение $x^2\equiv D \pmod{2^\lambda}$ всегда разрешимо, для всякого λ, если $D\equiv 1 \pmod 8$.

Установим число его корней; если $a^2\equiv D \pmod{2^\lambda}$ и $b^2\equiv D \pmod{2^\lambda}$, то $2^\lambda \mid (a+b)(a-b)$; a и b нечетные, поэтому $2^{\lambda-2} \mid \frac{a+b}{2}\cdot\frac{a-b}{2}$.

т. к. $a^2=2^\lambda+D$, D [illegible]

Из 2-х чисел $\frac{a+b}{2}$ и $\frac{a-b}{2}$ одно непременно четное, другое нечетное, т. е. $2^{\lambda-2} \mid \frac{a\pm b}{2}$ или $2^{\lambda-1} \mid a\pm b$. Значит или $b\equiv a \pmod{2^{\lambda-1}}$ или $b\equiv -a \pmod{2^{\lambda-1}}$.

Приведенные к модулю 2^λ, эти выражения дадут 4 корня:

$b\equiv a,\ a+2^{\lambda-1},\ -a,\ -a+2^{\lambda-1} \pmod{2^\lambda}$; эти корни несравнимы между собой.

V. $k = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_\varrho^{\lambda_\varrho}$, где $\varrho \geq 2$.

Мы видели, что, если дан ряд сравнений $x \equiv a_1 \pmod{k_1}$, $x \equiv a_2 \pmod{k_2}$ ... $x \equiv a_\varrho \pmod{k_\varrho}$, причем все модули попарно взаимно простые, то есть одно решение $(\mathrm{mod}\ k_1 k_2 \ldots k_\varrho)$, удовлетворяющее всем этим сравнениям.

Пусть наше сравнение $x^2 \equiv D \pmod{k = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_\varrho^{\lambda_\varrho}}$. Необходимое условие разрешимости этого сравнения заключается в том, что D должно быть вычетом чисел $p_1^{\lambda}, p_2, \ldots p_\varrho$.

Докажем, что это же условие достаточно. По приведенной выше теореме о системах сравнений (с степенями) существует класс чисел $(\mathrm{mod}\ k)$, удовлетворяющий всем этим сравнениям, причем за a_ν мы возьмем корень сравнения $x^2 \equiv D \pmod{p_\nu^{\lambda_\nu}}$. Этот класс и дает решение данного сравнения. Т.к. каждое из ϱ элементарных сравнений имеет 2 разных корня, то, комбинируя их всевозможными способами, мы получим 2^ϱ корней данного сравнения. Наше имеет или 0 или 2^ϱ корней. Помощью символов Лежандра это число выразится так:

$$\left[1+\left(\frac{D}{p_1}\right)\right]\left(1+\left(\frac{D}{p_2}\right)\right)\cdots\left(1+\left(\frac{D}{p_\varrho}\right)\right) = \prod_{p|k}\left(1+\left(\frac{D}{p}\right)\right).$$

IX

VI. $k = 2^\lambda p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_\varrho^{\lambda_\varrho}$, где $\lambda > 0$, $\varrho > 0$. Необходимое условие разрешимости сравнения: D должно быть квадратичным вычетом чисел $p_1, p_2, \ldots p_\varrho$. Рассмотрим случай

$\lambda = 1$. Тогда это условие необходимо и достаточно; число корней есть 2^ϱ.

$\lambda = 2$. Необходимое и достаточное условие, кроме предыдущих, следующее: $D \equiv 1 \pmod 4$. Число корней в этом случае $2^{\varrho+1}$.

$\lambda \geq 3$. Необходимо и дост. условія, кромѣ приведеннаго в 1-ом случаѣ, чтобы $D \equiv 1 \pmod 8$; тогда число корней будет $2^{\rho+2}$.

Переходим ко 2-ой задачѣ, связанной с сравненіями 2-ой степени.

Дано сравненіе $x^2 \equiv D \pmod K$, гдѣ D - данное число. Опредѣлить, при каких значеніях K это сравненіе разрѣшимо.

Полагаем $(D, K)=1$; $D = a.b.c\ldots$ - разложеніе на простые множители.

Положим, что K принимает значенія простого числа $K=p$.

Тогда $\left(\frac{D}{p}\right) = \left(\frac{a.b.c\ldots}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\ldots$

Рассмотрим отдѣльно 3 случая: $D=-1$, $D=2$, $D=q$ - нечетному простому числу. Всѣ остальныя значенія D получаются в видѣ произведеній этих трех основных типов.

1) $\left(\frac{-1}{p}\right) = \begin{cases} =1, \text{ если } p \equiv 1 \pmod 4 \\ =-1, \text{ если } p \equiv 3 \pmod 4 \end{cases}$

В самом дѣлѣ, по Эйлерову критерію, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ стр. 55, откуда и слѣдуют написанные равенства.

2) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ или $\begin{cases} =+1, \text{ если } p \equiv \pm 1 \pmod 8 \\ =-1, \text{ если } p \equiv \pm 3 \pmod 8 \end{cases}$

Оба эти опред. тождественны: в 1-ом случаѣ $p = 8n \pm 1$; — (нечет. степ.)

$\frac{p^2-1}{8} = \frac{64n^2 \pm 16n + 1 - 1}{8} = 8n^2 \pm 2n \equiv 0 \pmod 2$; во 2-ом случаѣ

$p = 8n \pm 3$; $\frac{p^2-1}{8} = \frac{64n^2 \pm 48n + 9 - 1}{8} = 8n^2 \pm 6n + 1 \equiv 1 \pmod 2$.

Доказ. Сначала докажем 2-ую ч. теоремы методом полной индукціи

Всѣ простыя числа в этом случаѣ имѣют вид $8n\pm3$; для 3 имѣем

$x^2\equiv 2 \pmod 3$ — сравненiе неразрѣшимо, по теор. Ферм. и наше утвержденiе вѣрно.

Допустим, что для нѣкотораго (наименьшаго) значенiя p, гдѣ $p=8n\pm3$, сравненiе

$x^2\equiv 2 \pmod p$ разрѣшимо. Тогда оно имѣет 2 корня между

0 и p; один четный, другой нечетный; пусть послѣднiй есть a.

$1\leq a\leq p-1$; $a^2-2=pf$, f — цѣлое число, нечетное; $f<p$, т. к.

лѣвая часть $<p^2$. ~~Если f простое числ~~ Т. к. квадрат нечетнаго

числа a сравним с 1 (mod 8), то $pf\equiv-1 \pmod 8$. Если $p\equiv\pm3$,

т. к. $p^2\equiv1 \pmod 8$ из пред.

то, на осн. пред. $f\equiv\mp3 \pmod 8$. Если f простое число, то мы

пришли к противорѣчiю, т. к. p не есть уже наименьшее простое число вида

$8n\pm3$, для котораго наше сравненiе разрѣшимо. Если же f

составное, то в числѣ его простых множителей должен быть

хоть один вида $8n\pm3$, для котораго наше сравненiе опять будет

разрѣшимо. И в этом случаѣ p не было бы наименьшим числом,

удовл. условiю. ~~Теор~~ 2ая часть теоремы доказана.

1ая часть. а) Дано $p\equiv-1 \pmod 8$, тр. док. $\left(\frac{2}{p}\right)=1$. Наименьшее простое число

указаннаго типа есть 7; для него ~~сравненiе~~ $\left(\frac{2}{7}\right)\equiv2^{\frac{7-1}{2}}=8\equiv1 \pmod 7$.

Пусть впервые для числа p разсматрив. типа $\left(\frac{2}{p}\right)=-1$. По преды-

дущему $\left(\frac{-1}{p}\right)=-1$, итак $\left(\frac{-2}{p}\right)=1$, т. е. сравненiе

$x^2+2\equiv0 \pmod p$ должно быть разрѣшимо. Один из корней, нечетный,

пусть будет a: $1\leq a\leq p-1$ и $a^2+2=pf$, гдѣ $0<f<p$, т. к. $pf\leq(p-1)^2+2=$

$=p^2-2p+3<p^2$, т. к. $p>7$. Мы имеем: $a^2+2\equiv 3 \pmod 8$, $p\equiv -1 \pmod 8$, след. $f\equiv -3 \pmod 8$. Итак $f=8n+5=\prod p'$. Очевидно, не все $p'\equiv 1$ или $3 \pmod 8$; есть хоть одно простое число $p' | f$ вида $8n+5$ или $8n+7$.
Если $p'=8n+5$, то сравнение $x^2+2\equiv 0 \pmod{p'}$ разрешимо, т. е. $\left(\frac{-2}{p'}\right)=1$; т. к. $\underbrace{\left(\frac{-1}{p'}\right)=1}_{\text{квадр.}}$, то, умножая символы, находим: $\left(\frac{2}{p'}\right)=1$. Т. обр. 2 было бы вычетом по модулю $p'=8n+5$, что противоречит доказанной части теоремы.
Если $p'=8n+7$, то p не есть наименьшее число этого вида, для которого утверждение теоремы неверно — противоречие.
(часть; в) $p=8n+1$. Имеем: $8 | p-1$. По предыдущему, сравнение $x^8-1\equiv 0 \pmod p$ имеет 8 корней; след. сравнение $x^4+1\equiv 0 \pmod p$ имеет 4 корня. ~~Значит~~ По доказанному, найдется такое число a ~~(квадрат корня этого сравнения)~~, что $a^4+1\equiv 0 \pmod p$ или $(a^2+1)^2-2a^2\equiv 0 \pmod p$. Следовательно $\left(\frac{2a^2}{p}\right)=1=\left(\frac{2}{p}\right)\left(\frac{a^2}{p}\right)=\left(\frac{2}{p}\right)$.
Теорема доказана для всех случаев.

3) $D=q$. Для исследования этого случая надо доказать теорему:

~~т. к. $\left(\frac{q}{p}\right)\equiv q^{\frac{p-1}{2}} \pmod p$.~~

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$ (Закон взаимности прост. чисел)

~~то~~ В раскрытом виде ~~условия~~ теорема утверждает:
1) Если $p\equiv 1 \pmod 4$, $q\equiv 1 \pmod 4$, то $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$; 2) Если $p\equiv 1 \pmod 4$, $q\equiv 3 \pmod 4$, то $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$; 3) если $p\equiv 3 \pmod 4$, $q\equiv 1 \pmod 4$, то $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$; 4) Если $p\equiv 3 \pmod 4$, $q\equiv 3 \pmod 4$, то $\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$.

Докажем предварительно лемму Гаусса

Д. Док. $\left(\frac{D}{p}\right)=(-1)^{\mu}$, где μ определяется следующим образом:

Возьмем ряд чисел: $D, 2D, \dots \frac{p-1}{2}D$ и найдем их наименьшие положительные вычеты (mod p); пусть λ из них $a_1, a_2, \dots a_\lambda < \frac{p}{2}$; остальные числом μ, $b_1, b_2, \dots b_\mu > \frac{p}{2}$. Т. обр. число μ определено. Очевидно $\lambda+\mu=\frac{p-1}{2}$.

Доказ. Перемножая с одной стороны, числа $D, 2D, \dots \frac{p-1}{2}D$, а с другой стороны их вычеты, имеем: $\left(\frac{p-1}{2}\right)! D^{\frac{p-1}{2}} \equiv a_1 a_2 \dots a_\lambda b_1 b_2 \dots b_\mu \pmod p$

Заменим числа b через $p-b$; тогда все числа $a_1, a_2, \dots a_\lambda, (p-b_1), \dots (p-b_\mu)$ лежат между 0 и $\frac{p}{2}$. Докажем, что между ними нет равных (mod p).

Допустим, что $a=p-b$; тогда было бы $CD \equiv p-C'D$, где $1 \le C \le \frac{p-1}{2}$, $1 \le C' \le \frac{p-1}{2}$; отсюда $C+C' \equiv 0 \pmod p$, что невозможно

Итак, наш последний ряд представляет, независимо от порядка, ряд чисел $1, 2, \dots, \frac{p-1}{2}$. Если так, то $a_1 a_2 \dots a_\lambda (-b_1)(-b_2)\dots(-b_\mu) D^{\frac{p-1}{2}} \equiv a_1 a_2 \dots a_\lambda b_1 b_2 \dots b_\mu \pmod p$

Сокращая находим: $D^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod p$, что и тр. док. или $\left(\frac{D}{p}\right)=(-1)^{\mu}$.

Доказательство теоремы:

Пусть p нечетное простое число, $q \neq p$ - любое простое число.

Пусть мы имеем: $q=q_1 p+r_1;\ 2q=q_2 p+r_2; \dots,\ \nu q=q_\nu p+r_\nu; \dots\ \frac{p-1}{2}q=q_{\frac{p-1}{2}} p+r_{\frac{p-1}{2}}$, (1)

где $1 \le r_\nu \le p-1$. Числа $r_1, r_2, \dots r_{\frac{p-1}{2}}$ суть $a_1, a_2, \dots a_\lambda, b_1, b_2, \dots b_\mu$ предыд. таблицы, а числа $1, 2, \dots \frac{p-1}{2}$ суть $a_1, a_2, \dots a_\lambda, p-b_1, p-b_2, \dots p-b_\mu$. Обозначим:

$\sum_{\nu=1}^{\lambda} a_\nu = A$, $\sum_1^{\mu} b = B$; тогда $\sum_{\nu=1}^{\frac{p-1}{2}} r_\nu = A+B$.

$1+2+\dots+\frac{p-1}{2} = \frac{\frac{p-1}{2}\cdot\frac{p+1}{2}}{2} = \frac{p^2-1}{8} = A+\mu p-B$. (2) Складываем равенства (1); имеем

$\frac{p^2-1}{8} q = p\sum_1 q_\nu + A + B$; вычитаем отсюда равенство (2).

$(q-1)\frac{p^2-1}{8} = p\sum_1 q_\nu + 2B - \mu p$; отсюда $\mu \equiv (q-1)\frac{p^2-1}{8} + \sum_1 q_\nu \pmod 2$

Разберем случай $q = 2$. Тогда $\mu \equiv \frac{p^2-1}{8} + \sum_1 q_\nu \pmod 2$. Но в этом случае все $q_\nu = 0$. Итак $\mu \equiv \frac{p^2-1}{8} \pmod 2$. По Гауссовой лемме отсюда следует, что $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$; т. к. $\left(\frac{p}{2}\right) = 1$, то для этого частного случая теорема доказана.

Пусть теперь q нечетное простое число. Мы имеем:

$q_\nu = \left[\frac{\nu q}{p}\right]$; $\mu \equiv \sum_{\nu=1}^{\frac{p-1}{2}} \left[\frac{\nu q}{p}\right] \pmod 2$. По лемме Гаусса

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{\nu=1}^{\frac{p-1}{2}}\left[\frac{\nu q}{p}\right]}$$; переменим роли p и q. Имеем:

$\left(\frac{p}{q}\right) = (-1)^{\sum_{\sigma=1}^{\frac{q-1}{2}}\left[\frac{\sigma p}{q}\right]}$. Перемножая эти формулы

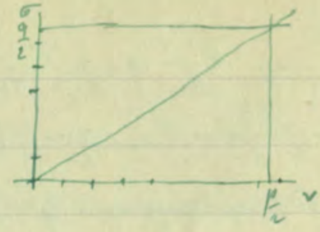
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{\nu=1}^{\frac{p-1}{2}}\left[\frac{\nu q}{p}\right] + \sum_{\sigma=1}^{\frac{q-1}{2}}\left[\frac{\sigma p}{q}\right]}.$$ Нам остается доказать,

что $\sum_{\nu=1}^{\frac{p-1}{2}}\left[\frac{\nu q}{p}\right] + \sum_{\sigma=1}^{\frac{q-1}{2}}\left[\frac{\sigma p}{q}\right] \equiv \frac{p-1}{2}\,\frac{q-1}{2} \pmod 2$

Берем разность $\frac{\sigma}{q} - \frac{\nu}{p}$; она $\neq 0$ (иначе мы имели бы $\sigma p = q\nu$, $p \mid \nu$, что невозможно, т. к. $\nu < p$). σ приним. значения $1, 2, \dots \frac{q-1}{2}$, ν также $1, 2, \dots \frac{p-1}{2}$. Общее число разностей есть $\frac{p-1}{2}\cdot\frac{q-1}{2}$. Из них положительны те, для кот. $\frac{\nu}{p} < \frac{\sigma}{q}$ или $\nu < \frac{\sigma p}{q} < \frac{p}{2}$. Их число соотв. знач. ν для данного σ есть $\left[\frac{\sigma p}{q}\right]$; число же всех положительных разностей есть $\sum_{\sigma=1}^{\frac{q-1}{2}}\left[\frac{\sigma p}{q}\right]$; точно также, докажем, что число отрицательных разностей есть $\sum_{\nu=1}^{\frac{p-1}{2}}\left[\frac{\nu q}{p}\right]$. Складывая, имеем $\sum_{\nu=1}^{\frac{p-1}{2}}\left[\frac{\nu q}{p}\right] + \sum_{\sigma=1}^{\frac{q-1}{2}}\left[\frac{\sigma p}{q}\right] =$ общ. ч. $= \frac{p-1}{2}\cdot\frac{q-1}{2}$.

Мы доказали даже равенство, а не сравнение.

Последнее доказательство хорошо иллюстрируется геометрически.



~~Воо~~ На оси ν отложим отрезки $1, 2, \dots \frac{p-1}{2}$. Проведем линію $\nu = \frac{p}{2}$; на оси σ отложим точки $1, 2, \dots \frac{q-1}{2}$ и проведем прямую $\sigma = \frac{q}{2}$. Проводим діагональ прямоугольника, уравненіе которой будет: $\frac{\sigma}{q} - \frac{\nu}{p} = 0$. Доказавши невозможность последняго равенства для цѣлых чисел σ и ν, мы покажем, что на діагонали не лежит ни одна точка с цѣлыми координатами. Для точек вниз от діагонали мы имѣем $\frac{\sigma}{q} - \frac{\nu}{p} < 0$, вверх от діагонали $\frac{\sigma}{q} - \frac{\nu}{p} > 0$. Число первых точек (цѣлых) есть $\sum_{\nu=1}^{\frac{p-1}{2}} \left[\frac{\nu q}{p}\right]$, число 2-ых есть $\sum_{\sigma=1}^{\frac{q-1}{2}} \left[\frac{\sigma p}{q}\right]$. Общее же число цѣлых точек в прямоугольникѣ есть $\frac{p-1}{2} \cdot \frac{q-1}{2}$.

Т. обр., на основаніи закона взаимности изученіе сравненія $x^2 \equiv q \pmod{p}$ при данном q мы сводим к изученію сравненія $x^2 \equiv p \pmod{q}$, гдѣ q дано, т. е. к 1-ой задачѣ сравненій 2-ой степени.

Примѣр. Изслѣдуем значеніе $\left(\frac{3}{p}\right)$; на осн. пред. $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$. Рассмотрим ~~просто~~ классы, взаимных простых с 12, чисел по (mod 12). В с. д. если простыя числа p и p' сравнимы (mod 12), то $\left(\frac{p}{3}\right) = \left(\frac{p'}{3}\right)$; с другой стороны $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p'-1}{2}}$. Слѣд. $\left(\frac{3}{p}\right) = \left(\frac{3}{p'}\right)$. Итак, изслѣдуем лишь простых чисел:

1) $p \equiv 1 \pmod{12}$, 2) $p \equiv 5 \pmod{12}$, 3) $p \equiv -5 \pmod{12}$; 4) $p \equiv -1 \pmod{12}$.

Примѣняя критерій Эйлера для выраженія $\left(\frac{p}{3}\right)$, мы найдем, что

$$\frac{3}{p} = \begin{cases} \text{в 1-ом случаѣ } +1, \text{ во 2-ом } -1 \\ \text{в 3-ем } -1, \text{ в 4-ом } +1. \end{cases}$$

причем, однако, мы не можем утверждать, что дѣйствит. существуют простыя числа всѣх этих 4-х классов

Якоби дал следующее обобщение символа Legendre'а:
определение

$\left(\frac{Q}{P}\right)$ имеет смысл для всякого P нечетного положительного и Q с ним взаимно просто. Если $P = pp'p''\dots$, то

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{p}\right)\left(\frac{Q}{p'}\right)\left(\frac{Q}{p''}\right)\dots = \prod_{p|P}\left(\frac{Q}{p}\right)$$

Свойства символа Якоби:

1) $\left(\frac{Q}{P_1}\right)\left(\frac{Q}{P_2}\right) = \left(\frac{Q}{P_1P_2}\right)$, как это видно легко из определения.

2) $\left(\frac{Q_1}{P}\right)\left(\frac{Q_2}{P}\right) = \left(\frac{Q_1Q_2}{P}\right)$. Доказ. $P = \prod p$; $\left(\frac{Q_1}{p}\right)\left(\frac{Q_2}{p}\right) = \left(\frac{Q_1Q_2}{p}\right)$ — симв. Leg. отсюда следует и теорема.

3) Если $Q_1 \equiv Q_2 \pmod P$, то $\left(\frac{Q_1}{P}\right) = \left(\frac{Q_2}{P}\right)$, т.к. $Q_1 \equiv Q_2 \pmod p$, где $p|P$

4) $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$; доказ. $\left(\frac{-1}{P}\right) = \left(\frac{-1}{p}\right)\left(\frac{-1}{p'}\right)\dots = (-1)^{\frac{p-1}{2}+\frac{p'-1}{2}+\dots}$. Остается доказ.
$\frac{p-1}{2} + \frac{p'-1}{2} + \dots \equiv \frac{pp'\dots-1}{2} \pmod 2$ или $(p-1)+(p'-1)+\dots \equiv pp'\dots - 1 \pmod 4$

Для 2 нечетных чисел u и v мы имеем: $(u-1)(v-1) \equiv 0 \pmod 4$ или $(u-1)+(v-1) \equiv uv-1 \pmod 4$

Для 3х неч. чисел $u(vw)-1 \equiv u-1+vw-1 \equiv (u-1)+(v-1)+(w-1) \pmod 4$ и т.д. Теор. док.

5) $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$. Доказ. $\left(\frac{2}{P}\right) = \left(\frac{2}{p}\right)\left(\frac{2}{p'}\right)\dots = (-1)^{\frac{p^2-1}{8}+\frac{p'^2-1}{8}+\dots}$. Докажем, что
$\frac{p^2-1}{8} + \frac{p'^2-1}{8} + \dots \equiv \frac{p^2p'^2\dots-1}{8} \pmod 2$ или $(p^2-1)+(p'^2-1)+\dots \equiv p^2p'^2\dots-1 \pmod{16}$.

Для 2х нечетных чисел u и v имеем: $(u^2-1)(v^2-1) \equiv 0 \pmod{64}$, т.е. $(u^2-1)+(v^2-1) \equiv u^2v^2-1 \pmod{64}$. Обобщение на n чисел очевидно.

6) Свойство взаимности. Если P и Q 2 положительных нечетных числа, то $\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$ или $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$.

Левая часть равна $\left\{\left(\frac{P}{q}\right)\left(\frac{P}{q'}\right)\dots\right\}\left\{\left(\frac{Q}{p}\right)\left(\frac{Q}{p'}\right)\dots\right\} = \left\{\left(\frac{p}{q}\right)\left(\frac{p'}{q}\right)\dots\left(\frac{p}{q'}\right)\left(\frac{p'}{q'}\right)\dots\right\}\left\{\left(\frac{q}{p}\right)\left(\frac{q'}{p}\right)\dots\left(\frac{q}{p'}\right)\left(\frac{q'}{p'}\right)\dots\right\}$

$= \prod\left(\frac{p}{q}\right)\cdot\prod\left(\frac{q}{p}\right) = \prod\left(\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\right) = \prod(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\sum_{p,q}\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\sum_p\frac{p-1}{2}\cdot\sum_q\frac{q-1}{2}} =$

Остается доказать $(-1)^{\Sigma_1 \frac{p-1}{2} \Sigma_1 \frac{q-1}{2}} = (-1)^{\frac{pp'\ldots-1}{2} \cdot \frac{qq'\ldots-1}{2}}$ или

$\Sigma_1 \frac{p-1}{2} \Sigma_1 \frac{q-1}{2} \equiv \frac{pp'\ldots-1}{2} \cdot \frac{qq'\ldots-1}{2} \pmod 2$. В теор. (4) доказано, что $\Sigma_1 \frac{p-1}{2} \equiv \frac{pp'\ldots-1}{2} \pmod 2$ и то же для q, откуда след. наше сравнение.

__Пример.__ 1) $\left(\frac{35}{281}\right) = \left(\frac{281}{35}\right) = \left(\frac{1}{35}\right) = +1$; 2) $\left(\frac{383}{443}\right) = -\left(\frac{443}{383}\right) = -\left(\frac{60}{383}\right) = -\left(\frac{15}{383}\right) = \left(\frac{383}{15}\right) = \left(\frac{8}{15}\right) = \left(\frac{2}{15}\right) = 1$ по теор. 5.

Решим 3-ю задачу в самом общем случае: определим значение $\left(\frac{D}{p}\right)$, где D — данное число, причем $p \nmid D$. Пусть $D = s^2 d$, где d уже не содержит квадратов; тогда $\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right)$. 2 случая:

1) d четное $d = 2e$, $e > 0$ и нечетное. $\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{e}{p}\right)$; если $e = 1$, то $\left(\frac{d}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Если $e \neq 1$, то $\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{e}\right)(-1)^{\frac{p-1}{2}\frac{e-1}{2}}$. При этом $\left(\frac{p}{e}\right) = \left(\frac{p'}{e}\right)$, если $p \equiv p' \pmod e$, а $\left(\frac{2}{p}\right) = \left(\frac{2}{p'}\right)$, если $p \equiv p' \pmod 8$; значит $\left(\frac{d}{p}\right) = \left(\frac{d}{p'}\right)$, если $p \equiv p' \pmod{8e = 4d}$.

2) d нечетное. $\left(\frac{d}{p}\right) = \left(\frac{p}{d}\right)(-1)^{\frac{p-1}{2}\frac{d-1}{2}}$. Если $d = 1$, то $\left(\frac{d}{p}\right) = +1$; пусть если $d \neq 1$.

Мы убедимся, что, если $p \equiv p' \pmod{4d}$, то $\left(\frac{d}{p}\right) = \left(\frac{d}{p'}\right)$ *)

Если D отрицательно, то $\left(\frac{D}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-D}{p}\right)$, где $-D$ положительно.

Период посл. символа $-4D$ или ~~и~~ $4D$.

Т. обр. ~~период~~ мы доказали периодичность функции $\left(\frac{D}{p}\right)$ относит. p, причем ея период $= 4D$ или ~~число~~ кратное $4d$, где если $D = s^2 d$.

*) ~~Все эти~~ Функция $\left(\frac{D}{p}\right)$ допускает период $4d$, подавно она допускает период $4D$.

W. Stepanoff.

Hilfssatz 1.

Zu jedem Exponenten m gehören eine gewisse Anzahl N positiver rationaler Zahlen

$$r_1, r_2, \dots, r_N,$$

sowie zwei positive ganze Zahlen a, A von folgender Eigenschaft:

es seien x und ξ beliebige positive ganze Zahlen und Γ eine beliebige reelle positive Zahl, es sei ferner X eine positive ganze Zahl, die der Ungleichung

$$X < \Gamma \xi^2 x^2$$

genügt; dann können zu diesen Grössen x, ξ, Γ, X stets N ganze Zahlen ($\gtreqless 0$)

$$X_1, X_2, \dots, X_N,$$

deren absolute Beträge den Ungleichungen

$$|X_h| < A\Gamma x \qquad (h = 1, \dots, N)$$

genügen, derart gefunden werden, dass die Gleichung

$$(\xi^2 x^2 + X)^m = \sum_{h=1,\dots,N} r_h (a\xi x + X_h)^{2m}$$

statthat.

Hilfssatz 2.

Zu jedem Exponenten m gehören wie in Hilfssatz 1 eine gewisse Anzahl N positiver rationaler Zahlen

$$r_1, r_2, \dots, r_N,$$

sowie zwei positive ganze Zahlen a, A von folgender Eigenschaft:

es seien x, ξ, Γ Zahlen wie in Hilfssatz 1, es sei ferner X eine positive ganze Zahl, die der Ungleichung

$$X < \Gamma^2 x^2$$

genügt, dann können zu diesen Grössen x, ξ, Γ, X stets N ganze Zahlen ($\geqq 0$)

$$X_1, X_2, \dots, X_N,$$

deren absolute Beträge den Ungleichungen

$$|X_h| < A\Gamma x \qquad (h = 1, \dots, N)$$

genügen, derart gefunden werden, dass die Gleichung

$$x(\xi^2 x^2 + X)^m = \frac{1}{\xi} \sum_{h=1,\dots,N} r_h (a\xi x + X_h)^{2m+1}$$

statthat.

Hilfssatz 3.

Zu jedem Exponenten m gehören eine gewisse Anzahl N positiver rationaler Zahlen

$$r_1, r_2, \ldots, r_N,$$ (von einer gewissen Stelle an) (def. für $1 \leqq \kappa < \frac{1}{2}\sqrt{K} - 1$)

ferner eine reelle, stets positive Funktion $\varphi(\kappa)$ der reellen Variabeln κ und endlich eine Funktion $F(K, \kappa)$ der ganzzahligen Variabeln K >16 und der reellen Variabeln κ, in denselben Grenzen die durchweg positive ganzzahlige Werte hat und bei festgehaltenem κ mit unendlich wachsendem K selbst, ohne je abzunehmen, über alle Grenzen wächst; diese zu m zugehörigen Grössen r_h, φ, F sind von folgender Beschaffenheit:

es sei x eine beliebige positive ganze Zahl und K eine beliebige positive ganze Zahl > 16, ferner κ eine reelle, der Ungleichung

$$1 \leqq \kappa < \frac{1}{2}\sqrt{K} - 1$$

genügende Grösse; es werde endlich

$$\kappa' = \varphi(\kappa), \quad K' = F(K, \kappa)$$

gesetzt. Wenn dann Y eine beliebige ganze Zahl ($\lesseqgtr 0$) ist, deren absoluter Betrag der Ungleichung

$$|Y| < \kappa \sqrt{K}\, x^2$$

genügt, so können zu diesen Grössen x, K, κ, Y stets N ganze Zahlen $Y_1', \ldots, Y_N'$ ($\lesseqgtr 0$), deren absolute Beträge die Ungleichungen

$$|Y_h'| < \kappa' \sqrt{K'}\, x$$

befriedigen, derart gefunden werden, dass die Gleichung

$$(Kx^2 + Y)^m = \sum_{h=1,\ldots,N} r_h (K'x + Y_h')^{2m}$$

stattfindet.

Hilfssatz 4.

Zu jedem Exponenten m gehören wie in Hilfssatz 3 eine gewisse Anzahl N positiver rationaler Zahlen

$$r_1, r_2, \dots, r_N,$$ Zahlen des Hilfsatzes 2

ferner eine reelle, stets positive Funktion $\varphi(\kappa)$ der reellen Variabeln κ und endlich eine Funktion $F(K, \kappa)$ der ganzzahligen Variabeln K und der reellen Variabeln κ, die durchweg positive ganzzahlige Werte hat und bei festgehaltenem κ mit unendlich wachsendem K selbst, ohne je abzunehmen, über alle Grenzen wächst; diese zu m zugehörigen Grössen r_h, φ, F sind von folgender Beschaffenheit:

Es seien x, K, κ Zahlen, die denselben Bedingungen wie in Hilfssatz 3 genügen; es werde endlich, wie dort

$$\kappa' = \varphi(\kappa), \quad K' = F(K, \kappa)$$

gesetzt; wenn dann Y eine beliebige ganze Zahl ($\gtreqless 0$) ist, deren absoluter Betrag der Ungleichung

$$|Y| < \kappa \sqrt{K}\, x^2$$

genügt, so können zu diesen Grössen x, K, κ, Y stets N ganze Zahlen $Y_1', \dots, Y_N'$ ($\gtreqless 0$), deren absolute Beträge die Ungleichungen

$$|Y_h'| < \kappa' \sqrt{K'}\, x$$

befriedigen, derart gefunden werden, dass die Gleichung

$$x(Kx^2+Y)^m = \frac{1}{K'} \sum_{h=1,\dots,N} r_h (K'x+Y_h')^{2m+1}$$

stattfindet.

Hilfssatz 5.

Zu jedem Exponenten n gehören zwei ganze Zahlen p, q, so dass
$$n = p + q$$
und
$$0 \leqq p < q$$
ist, ferner eine positive ganze Zahl K und eine gewisse Anzahl N^* positiver rationaler Zahlen
$$k_1, k_2, \ldots, k_{N^*}$$
von folgender Beschaffenheit:

ist x eine beliebige positive ganze Zahl, y irgend eine ganze Zahl ($\gtreqless 0$), deren absoluter Betrag der Ungleichung
$$|y| < \sqrt{K}\, x^q$$
genügt, so gibt es zu diesen Zahlen x, y stets gewisse N^* positive ganze Zahlen
$$\rho_1, \rho_2, \ldots, \rho_{N^*}$$
derart, dass die Gleichung
$$x^p (K x^q + y) = \sum_{h=1,2,\ldots,N^*} k_h \rho_h^n$$
statthat.

		Алг.	Тригон.
1)	Аргуновъ	9	13
2)	Был.	15	—
3)	Илера	17	3
4)	Иван.	3	5
5)	Ив-тих	10	12
6)	Ильинъ	7	11
7)	Кор.	6.	16
8)	Крав.	20	10
9)	Лавр.	18	14
10)	Левк.	8	—
11)	Рыбк.	13	2
12)	Роман.	1	17
13)	Поном.	12	15
	[illegible]	14	[illegible]

$1+\mathfrak{f}_{m+1} = \mathfrak{f}_{m}\, x - \frac{1}{2}\mathfrak{f}'_m$

$\mathfrak{f}_m = x^m - \binom{m}{2}\frac{1}{2}x^{m-2} + \binom{m}{4}\frac{1}{1}\frac{3}{2}x^{m-4}$

$\operatorname{sign} \mathfrak{f}_m(\beta_1) = (-1)^{m-1}$

$1-\frac{x}{a} = e^{-\frac{b}{2ma}}$

$\frac{x}{a} = 1 - e^{-\frac{b}{2ma}}$

$x = a\left(1-e^{-\frac{b}{2ma}}\right)$

$\frac{dy}{dx} = y^2$

$\frac{dy}{y^2} = dx$

$-\frac{1}{y} = x$

$\cancel{y' = y^2}$

$y = -\frac{1}{x}$ $y = e^{kx}$

$\cancel{e^{kx}\, k e^{kx} = e^{mx}}$

$f(y\,y') = 0$

$\cancel{y'' = y}$

$k^2 = 1$

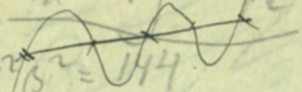
$\frac{e^x + e^{-x}}{}$

$y' = e^x - e^{-x}$

$e^x + e^{-x}$

$\cancel{x \cdot y = 144}$

$\frac{1}{\sqrt{x}} + \frac{1}{\sqrt{y}} = \frac{7}{12}$



$\alpha^2\beta^2 = 144$

$\frac{1}{\alpha} + \frac{1}{\beta} = 144$

$\frac{\alpha+\beta}{\alpha\beta} = \frac{7}{12}$

$\alpha + \beta = -7$

$xy = 144$

$\frac{1}{\sqrt{x}} + \frac{1}{\sqrt{y}} = \frac{7}{12}$

$\sqrt{x} = \alpha$

$\sqrt{y} = \beta$

$\frac{1}{\alpha} + \frac{1}{\beta} = \frac{7}{12}$

$\alpha\beta = 12$

$\sqrt{x} + \sqrt{y} = \ldots$

$\frac{1}{\sqrt{x}} - \frac{1}{\sqrt{y}} = \ldots$

$\underline{5, 9, 13 \ldots}$

10877

$10877 \mid 73$

73 | 149

357

392

657

657

$n = 73$

$\frac{a+u}{2} = 149$

$a = 298$

$n = 293$

$5 + x(72) = 293$

$72x = 288$

$xy' - by = \alpha + \beta x + \gamma x^2 y^2$

$\alpha + \beta x = \xi$

$\frac{dy}{dx} = \frac{dy}{d\xi}\,\beta$

$\cancel{\left(\frac{\xi - \alpha}{\beta}\right) y' \beta - by = \xi +}$

$\cancel{(\xi - \alpha)\, y'}$

$x - \alpha = \xi$

$y - \beta = \eta$

$\frac{dy}{dx} = \frac{dy}{d\xi} = \frac{d\eta}{d\xi}$

$\frac{dy}{dx} = \frac{A + ax + by}{B + a'x + b'y}$

$\frac{d\eta}{d\xi} = \frac{\alpha + b(\beta+\eta) +}{(\beta+\eta)}$

Глава 7. Теорія квадратичных формъ.

К теоріи квадратичных форм приводит нас рассмотрѣніе Діофантовского уравненія 2-ой степени:

$$ax^2+bxy+cy^2+dx+ey+f=0. \quad \text{(гдѣ коэф. цѣлыя числа)}$$

Разрѣшить это уравненіе в цѣлых числах значит найти всѣ точки с цѣлыми координатами, принадлежащія кривой 2-го порядка, выражаемой данным уравненіем. Случай $b=c=0$ приводит к параболѣ. Задача равносильна разрѣшенію сравненія 2-ой степени $ax^2+dx+f\equiv 0 \pmod e$, которым мы занимались в предыдущей главѣ. Перенося ~~центр~~ начало координат в центр кривой, мы приведем уравненіе к виду

$$ax^2+bxy+cy^2=k.$$

В связи с этим уравненіем возникают 2 задачи: 1) при данных a, b, c, k ~~~~ узнать путем конечнаго числа проб, разрѣшимо ли данное уравненіе в цѣлых числах; 2) при данных a, b, c узнать, какія числа k могут быть выражены квадратичной формой $ax^2+bxy+cy^2$, гдѣ x, y принимают цѣлыя значенія. Выраженіе b^2-4ac называется дискриминантом формы.

Теорема. Необходимое и достаточное условіе, чтобы форма распадалась на 2 линейные фактора с (раціональными) цѣлыми коэффиціентами, — дискриминант формы д. быть квадратным числом.

~~Доказ~~ Условіе необходимо. В. с. д. пусть

$ax^2+bxy+cy^2=(Ax+By)(Cx+Ey)$; сравнивая об[е] коэф., найдем:

$a=AC$, $b=AE+BC$, $c=BE$; $b^2-4ac=(AE+BC)^2-4A.C.BE=(AE-BC)^2$.

Доказано.

Условіе достаточно. Пусть

$$b^2-4ac=D=d^2$$

1 случай; $a=0$; разложеніе тривіальное: $y(bx+cy)$

2) $a\neq 0$. Умножаем об[е] части на $4a$, имеем:

$$4a(ax^2+bxy+cy^2)=(2ax+by)^2-d^2y^2=(2ax+(b+d)y)(2ax+(b-d)y).$$

или $ax^2+bxy+cy^2=\dfrac{(2ax+(b+d)y)(2ax+(b-d)y)}{4a}$.

Т.к., по опредѣленію, $d^2=b^2-4ac$, то $d\equiv b \pmod 2$. Всѣ коэффиціенты в скобках дѣлятся на 2, и мы имеем:

$$ax^2+bxy+cy^2=\frac{\left(ax+\frac{b+d}{2}y\right)\left(ax+\frac{b-d}{2}y\right)}{a}.$$

Чтобы доказать, что коэф. разложенія будут цѣлые, докажем лемму: Дано: $a\,|\,U.V$; тр. док.: можно представить $a=uv$, т.ч. $u\,|\,U$, $v\,|\,V$. Возьмем напримѣр $u=(a,U)$, $v=\dfrac{a}{(a,U)}$; нужно док. $v\,|\,V$; Мы имеем $a\,|\,U.V$. Дѣлим об[е] части на u;

$$\frac{a}{(a,U)}\,\Big|\,\frac{U}{(a,U)}.V;\ \text{т. к.}\ \left(\frac{a}{(a,U)},\frac{U}{(a,U)}\right)=1,\ \text{то}\ \frac{a}{(a,U)}\,\Big|\,V,\ \text{т. е.}\ v\,|\,V,\ \text{что и тр. док.}$$

На основаніи сказанного мы можем взять

$a=u.v$ так, что $u\,\big|\,\frac{b+d}{2}$, $v\,\big|\,\frac{b-d}{2}$. Дѣлим 1ую скобку на u, 2ую на v – и мы получим искомое разложеніе с цѣл. коэффиц.

Теор. доказана.

Наше уравненіе принимает вид: $(Ax+By)(Cx+Ey)=k$.

Разлагая k произв. образом на 2 целых фактора, мы получаем ряд систем $2^х$ лин. уравнений с $2^{мя}$ неизвестными. Этот случай не представляет большего интереса. Итак, будем предполагать D не квадратным числом.

Пусть дана форма

$$ax^2+bxy+cy^2$$

Ее дискриминант $D=b^2-4ac$.*) Рассмотрим случаи:

I. $D>0$. Форма — неопределенная, она может представлять, как положительные, так и отрицательные числа: В с. д., мы имеем:

$$4ak=(2ax+by)^2-Dy^2\text{; если } x=1,\ y=0\text{, то } 4ak>0$$

Если же положим $x=-b$, $y=2a$, то $4ak<0$.

II. $D<0$. Пусть $D=-\Delta$, где Δ полож.; $4ak=(2ax+by)^2+\Delta y^2$.

$2^{ая}$ часть существенно положительна (или $=0$). Значит форма может представлять только числа положительные (если a положит.) или только отрицательные (если a отриц.). При $x=y=0$ она представляет 0. Форма называется определенной.

Для определенной формы при данном k мы можем помощью конечного числа проб решить вопрос, возможно ли представить k в виде этой формы. В с. д. $4ak$ — данное число; $\Delta y^2 \leqq 4ak$, т. е.

*) Заметим, что наша форма может обладать целыми коэффициентами только в том случае, если $D\equiv 0 \pmod 4$ или $D\equiv 1 \pmod 4$
в четном — в нечетном

$|y| \leqq \sqrt{\frac{4ak}{\Delta}}$. Мы получили верхний предел $|y|$. Далее

$|2ax+by| \leqq \sqrt{4ak}$ – нам придется также испытать конечное число значений x.

Будем форму $ax^2+bxy+cy^2$ сокращенно обозначать через (a, b, c). Пусть числа a, b, c имеют общ. наиб. дел-теля s; очевидно s делит всякое число, представляемое этой формой. Докажем, что s будет общим наибольшим делителем всех чисел, представляемых формой. (Допустим, что общ. наиб. дел. всех чисел $t>s$). Положим сначала $x=1$, $y=0$; когда $k=a$; по предпол. $t|a$; затем положим $x=0$, $y=1$; $k=c$, $t|c$; положим $x=1$, $y=1$; $t|a+b+c$, так что $t|b$, что противоречит условию (s – общ. наиб. дел.)

Особен важен случай $s=1$. Тогда форма наз. первообразной (primitiv), в противном случае – непервообразной (imprimitiv).

Пусть имеем: $ax^2+bxy+cy^2=k$; если $(x,y)=1$, то k будет представлено собственно (eigentlich), в прот. случае – несобственно (uneigentlich)

Если $(x,y)=d>1$, то $a\left(\frac{x}{d}\right)^2+b\frac{x}{d}\cdot\frac{y}{d}+c\left(\frac{y}{d}\right)^2=\frac{k}{d^2}$ представит собственно число $\frac{k}{d^2}$. В последующем мы будем заниматься только собственными представлениями.

Пример. Форма x^2+y^2 представляет число 325 – во первых несобственно: $10^2+15^2=325$, во-вторых собственно $325=6^2+17^2$.

Пусть дана форма $\varphi = ax^2 + bxy + cy^2$. Введем новые переменные линейной подстановкой: $\left.\begin{array}{l} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y' \end{array}\right\}$ с целыми коэффициентами.

Тогда $\varphi = a(\alpha x' + \beta y')^2 + b(\alpha x' + \beta y')(\gamma x' + \delta y') + c(\gamma x' + \delta y')^2 = a'x'^2 + b'x'y' + c'y'^2$,

где $a' = a\alpha^2 + b\alpha\gamma + c\gamma^2$; $b' = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta$; $c' = a\beta^2 + b\beta\delta + c\delta^2$

Символически напишем это так:

$$(a, b, c) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} (a' b' c')$$

Пример. $\varphi = x^2 + y^2$; подстановка $\begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix}$; $\varphi = (x' + y')^2 + (2x' + 4y')^2 =$ $= 5x'^2 + 18x'y' + 17y'^2$. Символически $(1, 0, 1) \begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix} (5, 18, 17)$.

Выразим обратно ~~новые~~ переменные через старые; назовем $\alpha\delta - \beta\gamma = \varepsilon$; тогда $\varepsilon x' = \delta x - \beta y$, $\varepsilon y' = -\gamma x + \alpha y$; конечно $\varepsilon \neq 0$.

Чтобы x' и y' были всегда целыми числами при целых x и y, необходимо и достаточно иметь $\varepsilon = \pm 1$. Пусть $\varepsilon = 1$, т.е. $\alpha\delta - \beta\gamma = 1$; тогда

$$x' = \delta x - \beta y$$
$$y' = -\gamma x + \alpha y$$

$$\varphi(x, y) = ax^2 + bxy + cy^2 = a'x'^2 + b'x'y' + c'y'^2 = \psi(x', y').$$

Формы φ и ψ представляют одни и те же числа; они наз. эквивалентными. символ $\varphi \sim \psi$

3 основных теоремы об эквивалентных формах.

1) $\varphi \sim \varphi$. Доказ. Пусть $\varphi = ax^2 + bxy + cy^2$. Применим подстановку $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ с детерминантом 1. Тогда $x = x'$, $y = y'$; $\psi = ax'^2 + bx'y' + cy'^2$. Доказано.

2) Если $\varphi \sim \psi$, то $\psi \sim \varphi$. Пусть подстановка, переводящая φ в ψ, есть

$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ с детерм. 1. Обратно ψ переходит в φ посредством подстановки $\begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix}$, с детерминантом тоже $=1$. Доказано.

3) Дано: $\varphi\sim\varphi'$; $\varphi'\sim\varphi''$. Тр. док. $\varphi\sim\varphi''$. Пусть подстановка образующая φ в φ' есть:

$$x=\alpha x'+\beta y' \qquad \alpha\delta-\beta\gamma=1$$
$$y=\gamma x'+\delta y'$$

Подстановка, образ. φ' в φ'', есть

$$\left.\begin{aligned}x'&=\alpha' x''+\beta' y''\\ y'&=\gamma' x''+\delta' y''.\end{aligned}\right\}\alpha'\delta'-\beta'\gamma'=1$$

Подставляя 2-ая выраж. в 1-ую подстановку, находим:

$$x=\alpha(\alpha' x''+\beta' y'')+\beta(\gamma' x''+\delta' y'')=(\alpha\alpha'+\beta\gamma')x''+(\alpha\beta'+\beta\delta')y''$$
$$y=\gamma(\alpha' x''+\beta' y'')+\delta(\gamma' x''+\delta' y'')=(\gamma\alpha'+\delta\gamma')x''+(\gamma\beta'+\delta\delta')y''.$$

Вычислим детерминант этой подстановки

$$\begin{vmatrix}\alpha\alpha'+\beta\gamma', & \alpha\beta'+\beta\delta'\\ \gamma\alpha'+\delta\gamma', & \gamma\beta'+\delta\delta'\end{vmatrix}=\begin{vmatrix}\alpha & \beta\\ \gamma & \delta\end{vmatrix}\cdot\begin{vmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{vmatrix}=1,$$ причем умножение детерминантов в правой части происходит по правилу строки $\times$ столбцы.

Совокупность 4 чисел $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ при $\alpha\delta-\beta\gamma=1$ будем называть подстановкой.

Определим произведение 2-х подстановок следующим образом:

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{pmatrix}=\begin{pmatrix}\alpha\alpha'+\beta\gamma', & \alpha\beta'+\beta\delta'\\ \gamma\alpha'+\delta\gamma', & \gamma\beta'+\delta\delta'\end{pmatrix}.$$ Символически $S\cdot S'=S''$.

Произведение подстановок вообще не коммутативно; покажем это на примере. $S=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, $S'=\begin{pmatrix}1, & 0\\ -1, & 0\end{pmatrix}$. Перемножая, имеем:

$SS' = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$; $S'S = \begin{pmatrix}1 & 2\\ -1 & -1\end{pmatrix}$; получились разные результаты.

Ассоціативный закон имѣетъ мѣсто для подстановок.

Докажем, что $(SS')S'' = S(S'S'')$. Примѣняя подстановки послѣдовательно к кратным x, y, имѣем:

$\frac{x}{y} S \frac{x'}{y'} S' \frac{x''}{y''} S'' \frac{x'''}{y'''}$; очевидно мы имѣем $\frac{x}{y}(SS')\frac{x''}{y''}$, т.е. $\frac{x}{y}(SS')S''\frac{x'''}{y'''}$; с другой стороны $\frac{x'}{y'}(S'S'')\frac{x'''}{y'''}$, т.е. $\frac{x}{y}S(S'S'')\frac{x'''}{y'''}$

Теорема доказана.

Произведеніе любого числа подстановок $S_1 S_2 \dots S_n$ опредѣлено т. обр. вполнѣ, если дан порядок производителей.

Степень. $S^2 = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}^2 = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = \begin{pmatrix}\alpha^2+\beta\gamma, & \alpha\beta+\beta\delta\\ \alpha\gamma+\gamma\delta, & \beta\gamma+\delta^2\end{pmatrix}$

На основаніи ассоціативного закона имѣем:

$$S^{m+n} = S^m \,.\, S^n.$$

Для опредѣленія отриц. степеней назовем подстановкой $S^{-1} = \begin{pmatrix}\delta & -\beta\\ -\gamma & \alpha\end{pmatrix}$, если $S = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ и $\alpha\delta - \beta\gamma = 1$. Мы имѣем: $SS^{-1} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ тожественная подстановка $= E$. Точно также $S^{-1}S = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. Подстановка S^{-1} наз. обратной.

Докажем, что обратная подстановка единственная. Пусть $S.X = E$, т.е. $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}\lambda & \mu\\ \nu & \rho\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. Сравнивая, получим:

$$\left.\begin{aligned}\alpha\lambda+\beta\nu&=1\\ \alpha\mu+\beta\rho&=0\\ \gamma\lambda+\delta\nu&=0\\ \gamma\mu+\delta\rho&=1\end{aligned}\right\}$$

Рѣшая эти уравненія, получим 1 систему значеній λ, μ, ν, ρ. Легко показать, что тѣ же значенія λ, μ, ν, ρ получаются если исходить из равенства $XS = E$.

Указанные свойства композиционной подстановки:
$\mathcal{E}U=U$; в с.д. $\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}a&b\\c&d\end{pmatrix}$. Точно так же $U\mathcal{E}=U$.

Теорема. Эквивалентные формы имеют равные дискриминанты.

Дано: $\varphi=(a,b,c)\sim\psi=(a',b',c')$. Тр. док. $D=D'$, т.е. $b^2-4ac=b'^2-4a'c'$.

$b'^2-4a'c'=(2a\alpha\beta+b(\alpha\delta+\beta\gamma))^2-4(a\alpha^2+b\alpha\gamma+c\gamma^2)(a\beta^2+b\beta\delta+c\delta^2)=$
$a^2(4\alpha^2\beta^2-4\alpha^2\beta^2)+b^2($

что и тр. док.

Примеры эквивалентных форм:

1) $(a,b,c)\sim(c,-b,a)$. В с.д. при помощи подстановки $\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ т.е. $x=y'$, $y=-x'$ находим: $ax^2+bxy+cy^2=cx'^2-bx'y'+ay'^2$. Здесь можно также применить подстановку $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ или $x=-y'$, $y=x'$.

2) Применим к форме (a,b,c) подстановку $\begin{pmatrix}1&\beta\\0&1\end{pmatrix}$, где β — любое целое число. ~~Иначе~~ т.е. $x=x'+\beta y'$, $y=y'$. Форма примет вид:

$$a(x'+\beta y')^2+b(x'+\beta y')y'+cy'^2=ax'^2+(2a\beta+b)x'y'+(a\beta^2+b\beta+c)y'^2,$$ т.е.

$(a,b,c)\sim(a,2a\beta+b,a\beta^2+b\beta+c)$; ~~в част~~ заметим, что $b'\equiv b\pmod{2a}$

2 эквивалентных формы, в кот. 1ые коэффициенты одинаковы, а 2ые сравнимы между собою $\pmod{2a}$, наз. параллельными.

Теорема. Если зададим какое-ниб. Пусть дана форма (a,b,c) $b'\equiv b\pmod{2a}$, то всегда найдем целое c' такое, что форма $(a,b',c')\parallel(a,b,c)$.

Дск. $b'^2-4ac' = b^2-4ac = D$; $c' = \frac{b'^2-D}{4a} = \frac{(b+2\beta a)^2-D}{4a} = \frac{b^2-D}{4a}$ + нек. целое число.
т. к. $\frac{b^2-D}{4a}$ целое, теорема доказана.

3 основная теорема справедлива и для паралл. форм.

$1^{ое}$: ~~что~~ $\varphi \parallel \varphi$. – очевидно;

$2^{ое}$ Если $\varphi \parallel \psi$, то $\psi \parallel \varphi$; для доказательства применим к ψ подстановку $\begin{pmatrix} 1 & \frac{b'-b}{2a} \\ 0 & 1 \end{pmatrix}$; получим φ.

$3^{ье}$: Если $\varphi \parallel \varphi'$ и $\varphi' \parallel \varphi''$, то $\varphi \parallel \varphi''$.

<u>$3^{ий}$ пример</u>. Форма (a, b, c). Подстановка $\begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}$, где δ - целое число.
т. к. $x = y'$, $y = -x' + \delta y'$; форма перейдет в

$$ay'^2 + b(-x'+\delta y')y' + c(-x'+\delta y')^2; \quad (a, b, c) \sim (c, -b-2c\delta, a+b\delta+c\delta^2).$$

Заметим, что $a' = c$, $b + b' \equiv 0 \pmod{2c}$. Обратно, если дана (a, b, c) и $a' = c$, $b' + b \equiv 0 \pmod{2c}$, то найдется такое целое c', что $(a', b', c') \sim (a, b, c)$. В сам. деле $c' = \frac{b'^2-D}{4c} = \frac{(-b-2\delta c)^2-D}{4c} = \frac{b^2-D}{4c}$ + ц. число = целому числу. ~~Подстановки~~ Формы (a, b, c) и (a', b', c'), где $a' = c$ и $b + b' \equiv 0 \pmod{2c}$ – называются соседними (benachbart).

Заметим, что, ~~если~~ $(a, b, c)\begin{pmatrix} 0 & 1 \\ -1 & \frac{b+b'}{-2c} \end{pmatrix}(c, b', c')$, где $b + b' \equiv 0 \pmod{2c}$

Займемся исследованием разных форм, соответствующих данному дискриминанту D; заметим, что необходимо $D \equiv 0 \pmod 4$ или $D \equiv 1$.
Простейшая форма для $1^{го}$ случая есть $(1, 0, -\frac{D}{4})$, для $2^{го}$ $(1, 1, \frac{1-D}{4})$. Эти формы наз. главными формами.

Всякая главная форма представляет 1. Для этого достаточно положить $x=1$, $y=0$.

Докажем обратное: если форма представляет 1, то она эквивалентна главной форме. Пусть это форма (a,b,c).
Уравнение $1=a\alpha^2+b\alpha\gamma+c\gamma^2$ обладает след. по кр. мере одним решением. Т.к. мы занимаемся собственным представлением чисел, то $(\alpha,\gamma)=1$. На осн. теории сравнений при данных α и γ всегда можно найти пару целых чисел β,δ, удовлетворяющих уравнению $\alpha\delta-\beta\gamma=1$. Применим к (a,b,c) подстановку $\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}$. Получим:

$$(a,b,c)\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}(1,b',c').$$

Последнюю форму преобразуем в параллельную, в кот. $b''\equiv b' \pmod 2$. Если b' четное, то мы можем сделать $b''=0$; если b' нечетное, то будем иметь $b''=1$. Итак

$$(a,b,c)\begin{cases}\text{или} \sim (1,0,c'')\\ \text{или} \sim (1,1,c'')\end{cases}$$

, что и тр. док.

Т.к. $b^2-4ac=D$, то $b\equiv D \pmod 2$; Итак если D четно, форма приводится к 1-ому ~~нормальному~~ главному виду, если D нечетно — ко 2-ому.

<u>Теорема.</u> Пусть $k=ax^2+bxy+cy^2$ (предст. собственно). Тр. док., что (a,b,c) эквивалентно другой форме, где (где a,b,c,x,y — даны) 1-ый коэффициент есть k.
Решаем неопр. уравнение $x\eta-y\xi=1$; применяем подстановку

$$(a,b,c)\begin{pmatrix}x&\xi\\ y&\eta\end{pmatrix}(k,l,m),$$

что и тр. док.

Заметим, что $D=l^2-4km$; $l^2\equiv D \pmod{4k}$, т.е. D квадратичный вычет mod 4k. Т. обр. это условіе необходимое для того, чтобы (a, b, c) могла представлять число k.

Общее выраженіе чисел ξ' и η', удовлетворяющих ур-ію $x\eta - y\xi = 1$ есть $\xi' = \xi + xv$, $\eta' = \eta + yv$, гдѣ v цѣлое ~~число~~. Преобразуя получ. $(a, b, c)\begin{pmatrix} x & \xi' \\ y & \eta' \end{pmatrix}(k, l', m')$, причем

$$l' = 2ax\xi' + b(x\eta' + y\xi') + 2cy\eta' = 2ax(\xi + xv) + b\big(x(\eta + yv) + y(\xi + xv)\big) +$$
$$+ 2cy(\eta + yv) = l + v \cdot 2k,$$ т. е. $l' \equiv l \pmod{2k}$. (α)

Пусть нам дана форма (a, b, c) и число k; по предыдущему, (α) для l достаточно испробовать числа от 1 до $2|k|$, т. е. конечнаго числа испытаній. Тогда $m = \frac{l^2 - D}{4k}$, причем годятся только тѣ значенія l, для которых m получается цѣлое.

Поставим себѣ 2 проблемы. 1) Даны 2 формы φ и φ' с равными (одинаковыми) дискриминантами D; опредѣлить, эквивалентны ли онѣ и если да, то найти подстановку, переводящую одну форму в другую; 2) φ и φ' эквивалентны, извѣстна одна подстановка, опредѣлить всѣ остальныя.

Рѣшим 2-ую проблему. Данная подстановка S, одна из остальных S_1; $\varphi S \varphi'$, $\varphi S_1 \varphi'$; очевидно $\varphi' S_1^{-1} \varphi$; тогда $\varphi S S_1^{-1} \varphi$. Обозначим $S S_1^{-1} = R$. Имѣем $\varphi R \varphi$, т. е. R переводит форму φ

самое в себя. Если мы найдем R, то найдем S_1. Умножаем рав. $SS_1^{-1}=R$ в обеих частях справа на S_1; получим $SS_1^{-1}S_1=RS_1$ или $S=RS_1$; последнее равенство умножим в обеих частях слева на R^{-1}, $R^{-1}S=R^{-1}RS_1=S_1$. Так выражается S_1 через S и R.

Наша задача свелась к разысканию всех подстановок, преобразующих данную форму самое в себя. Решим эту задачу.

Отыскиваем коэф. $\alpha, \beta, \gamma, \delta$ подстановки R из след. уравнений:

$$(1)\qquad \alpha\delta-\beta\gamma=1$$

$$(2)\qquad a=a\alpha^2+b\alpha\gamma+c\gamma^2$$

$$(3)\qquad b=2a\alpha\beta+b(\alpha\delta+\beta\gamma)+2c\gamma\delta$$

$c=a\beta^2+b\beta\delta+c\delta^2$; одно решение этих уравнений мы знаем $\alpha=1, \beta=0, \gamma=0, \delta=1$ — но оно приводит к тождественной подстановке.

Последнее уравнение в дальнейшем не потребуется, т.к., если $(a,b,c)\sim(a',b',c')$, то $c'=c$. Пусть $\alpha,\beta,\gamma,\delta$ — решение 1ых 3 ур-ий.

Из (1) следует $\alpha\delta=\beta\gamma+1$; из (3) $b=2a\alpha\beta+b(\alpha\delta+\beta\gamma)+2c\gamma\delta$

$$(4)\qquad 0=a\alpha\beta+b\beta\gamma+c\gamma\delta$$

Из (4) и (2) исключаем b ((2)$\times\beta$, (4)$\times-\alpha$)

$$(5)\qquad a\beta=-c\gamma$$

Из (2) и (4) исключаем c ((2)$\times\delta$, (3)$\times-\gamma$)

$$(6)\qquad a\delta=a\alpha+b\gamma \qquad \text{или} \qquad a(\delta-\alpha)=b\gamma$$

Из (5) и (6) $a|b\gamma$, $a|c\gamma$, $a|(b,c)\gamma$, след. $a|\gamma$. Отсюда

$$(7)\quad a = \gamma u.$$

Вставляем в (5), делим на γ; находим

$$(8)\quad \beta = -cu.$$

Вставляем в уравнение (6)

$$(9)\quad \delta - \alpha = bu$$

Вставляем в (1) $\quad (10)\quad \alpha\delta = 1 - acu^2$

Для определения α и δ имеем ур-ия (9) и (10)

$(\delta+\alpha)^2 = (\delta-\alpha)^2 + 4\alpha\delta = b^2u^2 + 4 - 4acu^2 = 4 + Du^2$. = квадрат. числу

$$4 + Du^2 = t^2.$$

Значит, если $\alpha, \beta, \gamma, \delta$ – решения нашей системы, то u удовлетворяет последнему уравнению. ~~Одно решение его очевидно~~

Тогда найдем t. Получим

$$(11)\quad \delta + \alpha = t.$$

$\alpha = \frac{t - bu}{2}$, $\beta = -cu$, $\gamma = au$, $\delta = \frac{t + bu}{2}$.

Одно решение очевидно: $u = 0$, тогда $t = \pm 2$. Соответственно $\alpha = \pm 1$, $\beta = 0$, $\gamma = 0$, $\delta = \pm 1$. Мы нашли 2 подстановки, образующих форму самое в себя: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Докажем, что α и β в посл. формулах получаются целыми;

$t + Du \equiv 0 \pmod 2$, $b \equiv D \pmod 2$, т.е. $t \pm bu \equiv 0 \pmod 2$, что и тр. док.

Проверим, ~~что~~ полученные результаты, подставляя выражения $\alpha, \beta, \gamma, \delta$

в уравнения (1), (2), (3)

(1) $\alpha\delta - \beta\gamma = \frac{t^2 - b^2u^2}{4} + acu^2 = \frac{t^2}{4} - \frac{Du^2}{4} = 1.$

(2) $a\alpha^2 + b\alpha\gamma + c\gamma^2 = a\left(\frac{t-bu}{2}\right)^2 + b\left(\frac{t-bu}{2}\right)au + ca^2u^2 =$

$= \frac{a}{4}(t^2 - 2btu + b^2u^2 + 2btu - 2b^2u^2 + 4acu^2) = \frac{a}{4}(t^2 - Du^2) = a.$

(3) $2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = -a\,(t - bu)cu + b(1 - 2acu^2) +$
$+ cau(t + bu) = b.$

Итак, задача сведена к решению в целых числах уравнения

$$t^2 - Du^2 = 4.$$

Это последнее называется уравнением Pell'я.

Найдя решение Pell'евского уравнения (t, u), мы сейчас же напишем подстановку, преобразующую форму самое в себя. Это будет $\begin{pmatrix} \frac{t-bu}{2}, & -cu \\ au, & \frac{t+bu}{2} \end{pmatrix}$

Исследуем Pell'евское уравнение при $D<0$; обозначим $-D = \Delta > 0$.

Уравнение $t^2 + \Delta u^2 = 4$.

1 случай. $\Delta > 4$; тогда $u = 0$, $t = \pm 2$. Кроме 2-х тривиальных решений нет.

2) $\Delta = 4$. Ур. $t^2 + 4u^2 = 4$. Кроме тривиальных, имеем решение: $t = 0, u = \pm 1$

3) $\Delta = 3$; $t^2 + 3u^2 = 4$. Кроме 2-х тривиальных, имеем еще 4 решения.

$t = \pm 1$, $u = \pm 1$ (знаки независимы)

Затем исследуем уравнение при $D > 0$. ~~Это~~ Уравнение всегда имеет корни. Положим $t = 2x$, $u = 2y$, приведем уравнение к виду

$x^2 - Dy^2 = 1.$ (α)

Здѣсь D будемъ предполагать любымъ положит. числомъ, только не квадратнымъ. Докажемъ, что уравненіе всегда имѣетъ корни, кромѣ тривіальныхъ.

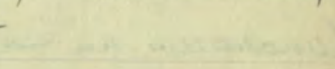
Лемма. Дано: $D>0$, не квадратъ; $m \geqq 1$ (ц. число). Тр. док.: Существуютъ такія цѣлыя $x>0$, $y>0$, $y \leqq m$, что $|x - y\sqrt{D}| < \frac{1}{m}$.

Возьмемъ для y рядъ значеній: $y_0 = 0, y_1 = 1, \dots y_m = m$. Опредѣлимъ затѣмъ y_μ и x_μ $(\mu = 0, 1, \dots m)$ такъ, чтобы

$$0 \leqq x_\mu - y_\mu\sqrt{D} < 1$$ или

$y_\mu\sqrt{D} \leqq x_\mu \leqq y_\mu\sqrt{D} + 1$. Если $\mu > 0$, то $x_\mu = [y_\mu\sqrt{D}] + 1$, для $\mu = 0$ $x_\mu = 0$.

Выраженіе $x_\mu - y_\mu\sqrt{D}$ получаетъ $m+1$ различныхъ значеній между 0 и 1; если этотъ промежутокъ разбить на m равныхъ частей (1-ая отъ 0 [включая нуль] до $\frac{1}{m}$, исключая $\frac{1}{m}$ и т.д.), то



по крайней мѣрѣ въ одномъ промежуткѣ окажется 2 значенія $x_\mu - y_\mu\sqrt{D}$; ихъ разстояніе (разность) $< \frac{1}{m}$.

Пусть это $x' - y'\sqrt{D}$ и $x'' - y''\sqrt{D}$; хоть одно изъ нихъ отлично отъ нуля. Вычитая, имѣемъ:
$$|x' - x'' - (y' - y'')\sqrt{D}| < \frac{1}{m}.$$

Пусть $y' > y''$. Полагаемъ $y' - y'' = y$, $x' - x'' = x$. Т.к. y' и $y'' \leqq m$, то $y' - y'' \geqq m$; x не можетъ быть 0; если бы $x \leqq 0$ то имѣли бы $|x - y\sqrt{D}| = -x + y\sqrt{D} \geqq y\sqrt{D} \geqq \sqrt{D} \geqq 1$, что против. ~~дан~~ требов. леммы.

Лемма доказана. Изъ нея непосредств. слѣдуетъ, что $|x - y\sqrt{D}| < \frac{1}{y}$.

2ая лемма. Существует бескон. число пар (x, y) таких, что $|x-y\sqrt{D}| < \frac{1}{y}$.

По предыдущему существует хотя одна такая пара x_0, y_0, что $|x^{(0)}-y^{(0)}\sqrt{D}| < \frac{1}{y^{(0)}}$. Выберем нат. ч. m' так, чтобы $\frac{1}{m'} < |x^{(0)}-y^{(0)}\sqrt{D}|$. Тогда существует такое $x'>0$, $0<y'\leq m'$, что

$$|x'-y'\sqrt{D}| < \frac{1}{m'} \leq \frac{1}{y'}$$

Т. обр. мы нашли 2ую пару (x', y'), удовлетворяющую данному неравенству. Затем опр. m'', т. что $\frac{1}{m''} < |x'-y'\sqrt{D}|$; находим $x''>0$, $0<y''\leq m''$, т. что $|x''-y''\sqrt{D}| < \frac{1}{m''} \leq \frac{1}{y''}$. Определяем 3ью пару (x'', y''); и т. д.

Доказательство теоремы. Берем (x, y) — одну из пар, удовлетворяющих последнему неравенству. Имеем:

$$0 < x+y\sqrt{D} = x-y\sqrt{D}+2y\sqrt{D} < \frac{1}{y}+2y\sqrt{D}$$

Умножаем на ~~нерав~~ $|x-y\sqrt{D}|$, кот. $< \frac{1}{y}$; получаем:

$$0 < |x^2-Dy^2| < \frac{1}{y^2}+2\sqrt{D} \leq 1+2\sqrt{D}.$$

Для наших пар (x, y) все значения x^2-Dy^2 суть целые числа заключенные в конечном промежутке от $-[1+2\sqrt{D}]$ до -1 и от $+1$ до $[1+2\sqrt{D}]$ ($x^2-Dy^2\neq 0$, т. к. D не квадратное число). Т. к. число пар бесконечно, а число целых чисел в указ. промежутке конечно, то найдется по кр. м. одно число нашего промежутка $k\neq 0$ такое, что уравнение $x^2-Dy^2=k$ удовлетворяется бесчисл. числом целых пар (x, y).

Распредѣлим всѣ x, y удовл. этому ур.-ію по классам mod $|k|$; это будут:

$x \equiv 0, 1, \ldots, |k|-1 \pmod{|k|}$; $y \equiv 0, 1, \ldots, |k|-1 \pmod{|k|}$

Число этих классов конечно, сл. есть хоть 1 класс $x^{ов}$ и хоть 1 класс $y^{ов}$ с безконечным числом элементов. Мы всегда можем выбрать 2 пары (x', y') и (x'', y'') так, что

$x'^2 - Dy'^2 = k$, $x''^2 - Dy''^2 = k$, и ~~притом~~ $x' \equiv x'' \pmod{|k|}$, $y' \equiv y'' \pmod{|k|}$, $x' \neq x''$, $y' \neq y''$; $x', x'', y', y'' > 0$.

Перемножаем 2 иррациональных числа

$(x' - y'\sqrt{D})(x'' + y''\sqrt{D}) = (x + y\sqrt{D})k$ т. е.

$kx = x'x'' - y'y''D \equiv x'^2 - Dy'^2 = k \equiv 0 \pmod{|k|}$

$ky = x'y'' - y'x'' \equiv x'y' - y'x' \equiv 0 \pmod{|k|}$; y и x — цѣлыя числа.

Замѣняем $\sqrt{D}$ на $-\sqrt{D}$; получаем:

$(x' + y'\sqrt{D})(x'' - y''\sqrt{D}) = (x - y\sqrt{D})\, k$.

Перемножаем последнія уравненія:

$$(x'^2 - Dy'^2)(x''^2 - Dy''^2) = (x^2 - Dy^2)\, k^2 \text{ или}$$

$k \cdot k = (x^2 - Dy^2) k^2$; $x^2 - Dy^2 = 1$.

Мы нашли одну пару, удовлетворяющую уравненію. Остается доказать, что рѣшеніе не тривіальное, т. е. мы не имѣем значеній $x = \pm 1$, $y = 0$. Допустим, что $x = \pm 1$, $y = 0$. Тогда

$kx = x'x'' - Dy'y'' = \pm k$; $ky = x'y'' - x''y' = 0$; умн. 1-ое на y''.

$\pm ky'' = -Dy'y''^2 + y'x''^2 = ky'$; т. е. $\pm y'' = y'$ или $y'' = y'$, а это против. невозможно.

Возвращаемся к Пеллевскому уравнению $t^2-Du^2=4$. Берем одно из его положит. решений (не тривиальное) $t_0>0$, $u_0>0$. Ему соответствует 4 решения $\pm t_0, \pm u_0$. Составим иррац. выражение $\frac{t_0+u_0\sqrt{D}}{2}$. Если $t_0>0$, $u_0>0$, то $\frac{t_0+u_0\sqrt{D}}{2} \geqq \frac{1+1.\sqrt{D}}{2} > 1$. Чтобы найти пределы $\frac{t_0-u_0\sqrt{D}}{2}$, замечаем, что $\frac{t_0+u_0\sqrt{D}}{2}\cdot\frac{t_0-u_0\sqrt{D}}{2}=1$, т. е. $\frac{t_0-u_0\sqrt{D}}{2}<1$.

Умножая неравенства на -1, найдем пределы для $\frac{-t_0+u_0\sqrt{D}}{2}$ и $\frac{-t_0-u_0\sqrt{D}}{2}$. Мы видим, что 4 иррац. числа $\frac{-t_0-u_0\sqrt{D}}{2}$, $\frac{-t_0+u_0\sqrt{D}}{2}$, $\frac{t_0-u_0\sqrt{D}}{2}$ и $\frac{t_0+u_0\sqrt{D}}{2}$ лежат соответственно в промежутках: $-\infty\ldots-1$; $-1\ldots0$; $0\ldots+1$; $+1\ldots+\infty$.

$--$, $-+$, $+-$, $++$

-1 $\quad 0$ $\quad +1$

Пусть (t', u'), (t'', u'') суть решения уравнения. Составляем выражения

$$\frac{t'+u'\sqrt{D}}{2}\cdot\frac{t''+u''\sqrt{D}}{2}=\frac{t+u\sqrt{D}}{2}.$$

Докажем, что t, u тоже решения уравнения. $t=\frac{t't''+Du'u''}{2}$; $u=\frac{t'u''+u't''}{2}$.

$t'^2-Du'^2=4$; откуда $t'+Du'\equiv 0 \pmod 2$ или $t'\equiv Du' \pmod 2$

$t't''+Du'u''\equiv Du'Du''+Du'u''=Du'u''(D+1)\equiv 0 \pmod 2$. Значит t — целое ч.

$t'u''+t''u'\equiv Du'u''+Du'u''\equiv 0 \pmod 2$, т. е. u — целое число.

Заменяем $\sqrt{D}$ через $-\sqrt{D}$.

$\frac{t'-u'\sqrt{D}}{2}\cdot\frac{t''-u''\sqrt{D}}{2}=\frac{t-u\sqrt{D}}{2}$. Перемножаем: $1=\frac{t^2-Du^2}{4}$; t и u действительно удовлетворяют уравнению.

Пусть T, U — решение уравнения. $\left(\frac{T+U\sqrt{D}}{2}\right)^n=\frac{t+u\sqrt{D}}{2}$. По доказанному t, u тоже решение уравнения. (Pell'а)

Пусть T, U есть наименьшее полож. рѣшеніе, т. е. рѣшеніе в кот. U имѣет самое малое полож. значеніе.

Докажем теорему: всѣ рѣшенія (t, u) даны формулой $\pm\left(\frac{T+U\sqrt{D}}{2}\right)^n = \frac{t+u\sqrt{D}}{2}$; в частности и знак + при $n=0$ имѣем тривіальное рѣшенія, при $n \geq 1$ рѣшенія, для кот. $\frac{t+u\sqrt{D}}{2} > 1$, при $n \leq 1$ т. к. $\frac{t+u\sqrt{D}}{2} < 1$ и соотвѣтственно для знака −.

Пусть $\frac{t+u\sqrt{D}}{2} > 1$. Тр. док., что это выраженіе — положит. степень от $\frac{T+U\sqrt{D}}{2}$. Допустив обратное, имѣем:

$$\left(\frac{T+U\sqrt{D}}{2}\right)^n < \frac{t+u\sqrt{D}}{2} < \left(\frac{T+U\sqrt{D}}{2}\right)^{n+1}, \text{ гдѣ } n \geq 0.$$

Умножаем обѣ части на $\left(\frac{T-U\sqrt{D}}{2}\right)^n$; замѣтим, что $\frac{t+u\sqrt{D}}{2}\left(\frac{T-U\sqrt{D}}{2}\right)^n = \frac{t'+u'\sqrt{D}}{2}$, гдѣ (t', u') тоже рѣшеніе.

Имѣем: $1 < \frac{t'+u'\sqrt{D}}{2} < \frac{T+U\sqrt{D}}{2}$, т. е. $t' < T$, $u' < U$; $t' > 0, u' > 0$, тогда (T, U) не было бы наименьшим рѣшеніем — против условія.

Мы доказали, что всѣ рѣшенія заключены в формулѣ $\pm\left(\frac{T+U\sqrt{D}}{2}\right)^n$, гдѣ n — любое цѣлое число.

Примѣр. $D=5$. Уравненіе $t^2-5u^2=4$. Наименьшее рѣшеніе $T=3, U=1$. Положим $n=2$; $\left(\frac{3+\sqrt{5}}{2}\right)^2 = \frac{14+6\sqrt{5}}{4} = \frac{7+3\sqrt{5}}{2}$; слѣдующее рѣшеніе $t=7, u=3$.

Для положительных значеній n имѣем формулу:

$$t = \left(\frac{T+U\sqrt{D}}{2}\right)^n + \left(\frac{T-U\sqrt{D}}{2}\right)^n = \frac{T^n + \binom{n}{2}T^{n-2}U^2D + \binom{n}{4}T^{n-4}U^4D^2 + \dots}{2^{n-1}}$$

$$u = \frac{1}{\sqrt{D}}\left[\left(\frac{T+U\sqrt{D}}{2}\right)^n - \left(\frac{T-U\sqrt{D}}{2}\right)^n\right] = \frac{\binom{n}{1}T^{n-1}U + \binom{n}{3}T^{n-3}U^3D + \dots}{2^{n-1}}$$

Обозначим $R=\begin{pmatrix}\frac{t-bu}{2}, & -cu \\ au, & \frac{t+bu}{2}\end{pmatrix}$. Пусть $\varphi S \psi$, гдѣ S извѣстная подстановка; тогда всѣ остальныя подстановки, переводящія φ в ψ, даны формулой RS. Т. обр. 2ая проблема (теоріи) из нами поставленных разрѣшена вполнѣ.

Примѣним полученные результаты к разрѣшенію вопроса: найти всѣ собственныя изображенія даннаго ~~числа~~ k помощью данной (a,b,c) формы. Мы видѣли, что всѣ подстановки, переводящія форму (a,b,c) в (k,l,m) имѣют вид $\begin{pmatrix}x & \xi \\ y & \eta\end{pmatrix}$, гдѣ ξ, η удовлетворяют уравненію $x\eta - y\xi = 1$. На основаніи предыдущаго, если $\begin{pmatrix}x_0 & \xi_0 \\ y_0 & \eta_0\end{pmatrix}$ одна из таких подстановок, то всѣ остальныя получатся в видѣ

$$\begin{pmatrix}x & \xi \\ y & \eta\end{pmatrix}=\begin{pmatrix}\frac{t-bu}{2}, & -cu \\ au, & \frac{t+bu}{2}\end{pmatrix}\begin{pmatrix}x_0 & \xi_0 \\ y_0 & \eta_0\end{pmatrix}$$

Отсюда имѣем:

$$x=\frac{t-bu}{2}x_0-cuy_0\ ;\quad y=aux_0+\frac{t+bu}{2}y_0.$$

Эти формулы дают всѣ пары (x,y), удовлетворяющія соотношенію $ax^2+bxy+cy^2=k$, если извѣстна одна пара x_0, y_0, удовлетворяющая этому соотношенію. Если $(x_0,y_0)=1$, то и $(x,y)=1$, т. е. мы получим только собственныя изображенія.

Перейдем к 1ой проблемѣ: даны 2 формы с равными дискриминантами; рѣшить, эквивалентны ли, когда онѣ

(стр. 52)

где $x^2 \equiv D \pmod 4$ следует

$x^2 = D + 4v$, где $(D, 4) = 1$.

т.е. D неч. число вида или

$2k+1$, $4k+1$, ...

или $2k \mp 1$, $4k \mp 3$. ...

если бы $D = 2k+1$, то

$x^2 = 4v + 2k + 1 = 2l + 1$

ясно, что если x^2 неч., то и

x неч., ибо если бы x было

четно, напр. $2y$, то $x^2 = 4y$

что, что-же четно.), следов.

x неч., и значит $x = 2n+1$

откуда $x^2 = 4m+1$, а у ~~нас~~

мы предпол. что $x^2 = 2l+1$

это весьма очевидно неверно

а значит предп. что $D = 2k+1$

неверно; далее если бы

было $D = 4k+3$, (или $D = 4k-1$)

то $x^2 = 4v + 4k + 3 = 4l + 3$

но $x^2 = 4n+1$ и очевидно, такое

неверно, что необх. должно быть

$$D \equiv 1 \pmod 4$$

чтобы сравнение имело

смыслъ

(стр 52) (Л. Г. Ландау) Л. Л.

Исследуем случай: $D<0$, т. е. форма определенная; они будут определенными положительными, если $a, c>0$ и опр. отрицательными, если $a, c<0$. Очевидно, нам достаточно исследовать определенно положительные формы.

Теорема. Число не эквивалентных классов в этом случае конечно. Пусть (a_0, b_0, c_0) произвольная форма с $D<0$. Существует наименьшее положительное число a_1, которое она представляет; соответствующие значения x, y пусть будут α, γ. Тогда

$$a_1 = a_0\alpha^2 + b_0\alpha\gamma + c_0\gamma^2$$

Очевидно $(\alpha, \gamma)=1$, т.к. иначе наименьшее число, представляемое формой $\frac{a_1}{d^2}$. Выбираем β и δ, удовлетворяющие уравнению: $\alpha\delta - \beta\gamma = 1$. Получаем:

$$(a_0, b_0, c_0)\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}(a_1, b_1, c_1).$$

Переводим последнюю форму в параллельную:

$$(a_1, b_1, c_1)\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}(a_1, b_2, c_2), \text{ где } b_2 \equiv b_1 \pmod{2a_1}.$$

и $\beta = \frac{b_2 - b_1}{2a_1}$. Выбираем для b_2 наименьшее по абсолютной величине значение; $-a_1 \leqq b_2 \leqq a_1$. Итак, мы имеем $(a_0, b_0, c_0)\sim(a', b', c')$, где a' - наименьшее число, представляемое данной формой, $|b'| \leqq a' \leqq c'$, т.к. и c' может быть представлено данной формой. Формы типа (a', b', c')

будем называть приведенными формами. Если разбить все формы данного дискриминанта $D<0$ на неэквивалентные классы, то в каждом классе будет по кр. мере одна приведенная форма.

Докажем, что существует конечное число приведенных форм (данного дискриминанта). Обозначим $-D=\Delta>0$.

$4ac-b^2=\Delta$, где $\Delta\equiv 3$ или $4 \pmod 4$ (в нечт. в четн.). Тр. док., что число систем a, b, c, удовлетворяющих этому равенству и неравенствам $|b|\leqq a\leqq c$ — конечно. Мы имеем:

$$4a^2\leqq 4ac=b^2+\Delta\leqq a^2+\Delta, \text{ откуда}$$

$3a^2\leqq\Delta$, $a\leqq\sqrt{\frac{\Delta}{3}}$. Существует конечное число целых и пол. значений a, удовлетворяющих этому неравенству. Т. к. $|b|\leqq a$, то $|b|\leqq\sqrt{\frac{\Delta}{3}}$; этому неравенству удовлетворяет конечное число целых значений b; $b=0, 1,\ldots\left[\sqrt{\frac{\Delta}{3}}\right]; -1,-2,\ldots,-\left[\sqrt{\frac{\Delta}{3}}\right]$.

Из конечного числа значений a и b надо выбрать только те, которые дают для $c=\frac{\Delta+b^2}{4a}$ значения целые и $\geqq a$. Т. обр. мы получим конечное число приведенных форм данного дискриминанта D. ~~Теорема доказана~~ ~~Остается решить вопрос, не будет ли между пр~~ Теорема доказана, т. к. очевидно, число неэквивал. классов $\leqq$ числу приведенных форм.

Решим вопрос, когда 2 приведенных формы эквивалентны

Рассмотрим предварительно 2 случая:

1) Приведенные формы $(a, a, c) \sim (a, -a, c)$. В самом деле

$$(a,a,c) \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} (a, -a, c)$$

2) $(a, b, a) \sim (a, -b, a)$, т.к. $(a, b, c) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} (c, -b, a)$

Теорема. Кроме двух ~~приведенных~~ указанных случаев, приведенные формы никогда не эквивалентны.

Дано: прив. ф. $(a, b, c) \sim (a', b', c')$. Тр. док.: или $a'=a$, $b'=b$, или $a'=a$, $b^*=a$, $b'=-a$ (или, что то же, $a'=a$, $b'=a$, $b=-a$) или, наконец, $a'=a$, $b'=-b$, $c=a$.

Положим, $a' \leqq a$. Напишем соотношения между коэф. форм.

$$a'=a\alpha^2+b\alpha\gamma+c\gamma^2 \qquad (4a)$$
$$b'=2a\alpha\beta+b(\alpha\delta+\beta\gamma)+2c\gamma\delta$$
$$\alpha\delta-\beta\gamma=1.$$

Из 1-го следует: $4aa'=(2a\alpha+b\gamma)^2+\Delta\gamma^2 \leqq \frac{4\Delta}{3}$

Разберем случаи: I. $\gamma=0$; $\alpha\delta=1$; $\alpha=\delta=\pm 1$. 2-ое уравнение даст

$$b'=2a\alpha\beta+b=\pm 2a\beta+b \; ; \text{ из 1-го } a'=a$$

$|b'| \leqq a'=a$, $|b| \leqq a$; b и b' лежат между $-a$ и $+a$ включительно. $2a \mid b-b'$. Значит, или $b^*=-a$, $b'=a$ или $b=a$, $b'=-a$ (2-ое условие теоремы) или $b=b'$ – тривиальный случай.

II. $\gamma=\pm 1$; $a'=a\alpha^2 \pm b\alpha+c \leqq a$; $a\alpha^2 \pm b\alpha \leqq a-c$; $|b| \leqq a$; $|\alpha| \leqq \alpha^2$, т.е. $|b\alpha| \leqq a\alpha^2$. Значит $a\alpha^2 \pm b\alpha=0$. Отсюда следует $a'=c \leqq a$. Но

$c \geqq a$, слѣд. $\underline{c=a}$; $b' = \underline{2a\alpha\beta} + b(2\alpha\delta - 1) + \underline{2c\gamma\delta}$. Отсюда
$b' \equiv b(2\alpha\delta-1) \pmod{2a}$, но $a \mid \beta\alpha$, значит $b' \equiv -b \pmod{2a}$
$|b'| \leqq a'$, $|b'| \leqq a$; также $|b| \leqq a$. Представляются случаи:
1) $b = a$, $-b' = -a$; 2) $b = -a$, $-b' = a$ — тривіальные случаи.
3) $b = -b'$ — послѣдній случай в условіи теоремы.
Теорема доказана.
Мы можем выбрать нѣкоторое число приведенных форм за представителей неэквивалентных классов.
Если даны 2 формы φ и ψ, то вопрос об их эквивалентности рѣшается так: ищем приведенную форму, $\sim \varphi$ и прив. форму $\sim \psi$. Если онѣ тождественны или эквивалентны, то $\varphi \sim \psi$.

Переходим к изслѣдованію эквивалентности неопредѣленных форм, т.е. к случаю $D > 0$. Опредѣлим для этого случая понятіе приведенной формы. Форма (a, b, c) называется приведенной, если $b < \sqrt{D}$; $\sqrt{D} - b < 2|a| < \sqrt{D} + b$.

Теорема. Существует конечное число приведенных форм данного дискриминанта $D > 0$.
Из $2^{го}$ опредѣленія приведенной формы имѣем: $b > 0$; т.к. $b < \sqrt{D}$, то существует только конечное число подходящих значеній b.
Далѣе $b^2 - 4ac = D$, $4ac = b^2 - D$; значит, существует только конечное

число значений a и c, удовлетворяющих условиям. Теорема доказана.

Теорема. В каждом классе эквивалентных форм есть хоть одна приведенная.

Пусть $\varphi=(a_0, b_0, a_1)$ есть любая форма дискрим. D. Пишем форму соседнюю справа $\varphi_1=(a_1, b_1, a_2)$, где $\varphi\begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}\varphi_1$; $\delta=-\frac{b_0+b_1}{2a_1}$ если $b_1\equiv -b_0 \pmod{2|a_1|}$. На каждом промежутке длины $|2a_1|$ лежит одно значение b_1. Выберем b_1 так, чтобы $\sqrt{D}>b_1>\sqrt{D}-2|a_1|$, т.е. b_1 = одному из чисел: $[\sqrt{D}], [\sqrt{D}]-1, \dots, [\sqrt{D}]-2|a_1|+1$.

1 случай: $|a_1|\leqq|a_2|$, тогда φ_1 есть привед. форма. В с.д. неравенство $\sqrt{D}-b_1<|2a_1|$ выполнено благодаря выбору b_1; кр. того имеем $b_1<\sqrt{D}$. $b_1^2-D=4a_1a_2$; $|D-b_1^2|=4|a_1||a_2|\geqq 4|a_1|^2$ или $|\sqrt{D}+b_1|(\sqrt{D}-b_1)\geqq 2|a_1|.2|a_1|$. 2-ой фактор слева $<$ 2-го фактора справа, след. $|\sqrt{D}+b_1|>2|a_1|>\sqrt{D}-b_1$. Отсюда следует: $b_1>0$ и $\sqrt{D}+b_1>2|a_1|$. Значит форма φ_1 действ. приведенная.

2-ой случай. Если $|a_1|>|a_2|$, то ищем правого соседа к φ_1. Это будет $\varphi_2=(a_2, b_2, a_3)$, где $\sqrt{D}>b_2>\sqrt{D}-2|a_2|$; случай 2а) $|a_2|\leqq|a_3|$; тогда φ_2 по доказанному, приведенная форма. Случай 2в). $|a_2|>|a_3|$, тогда ищем правого соседа к φ_2 и т.д. Мы получим: $|a_1|>|a_2|>|a_3|\dots$. Процесс должен окончиться, т.к. ряд убывающих положит. чисел не бесконечен, и мы непременно дойдем до приведенной формы.

Теорема. В приведенной форме $ac<0$. В с.д. $b^2-4ac=D$; $4ac=b^2-D<0$, что и т. доп.

Теорема. В прив. форме $\sqrt{D}-b<2|c|<\sqrt{D}+b$. Док. $D-b^2=-4ac=2|a|.2|c|$;

$(\sqrt{D}+b)(\sqrt{D}-b)=2|a|\cdot 2|c|$. Т.к. $\sqrt{D}-b<2|a|$, то $\sqrt{D}+b>2|c|$; т.к. $\sqrt{D}+b>2|a|$, то $\sqrt{D}-b<2|c|$, что и тр. док.

Теорема. Каждая приведенная форма имеет соседнюю справа одну и только одну приведенную эквивалентную ей форму.

Пусть $\varphi=(a\; b\; a_1)$ привед. форма. Берем форму соседнюю справа $\varphi_1=(a_1, b_1, a_2)$, где $b_1\equiv -b \pmod{2|a_1|}$ и так, чтобы $\sqrt{D}>b_1>\sqrt{D}-2|a_1|$. ~~Соответственно~~ b_1 определено т. обр. однозначно. Докажем, что φ_1 - приведенная форма, т.е. $\sqrt{D}-b_1<2|a_1|<\sqrt{D}+b_1$; 2-ая часть выполняется. Рассмотрим 2 случая.

1) $2|a_1|>\sqrt{D}$. Тогда $b_1=2|a_1|-b$. В с.д. $\sqrt{D}-b<2|c|<\sqrt{D}+b$ или в нашем сл. $\sqrt{D}-b<2|a_1|<\sqrt{D}+b$, откуда $\sqrt{D}>2|a_1|-b$, ~~$\sqrt{D}>b_1$~~. Остается доказать, что $2|a_1|-b>\sqrt{D}-2|a_1|$. Последнее неравенство выполняется, т.к. правая ч. отрицательна, а левая положительна, ибо $b<\sqrt{D}<2|a_1|$.

2) $2|a_1|<\sqrt{D}$; отсюда, т.к. $\sqrt{D}>b_1>\sqrt{D}-2|a_1|$, имеем:

$$2|a_1|-b_1<\sqrt{D}-(\sqrt{D}-2|a_1|)=2|a_1|<\sqrt{D}.$$

Т. обр. мы доказали, что φ_1 прив. форма.

Итак мы имеем $\varphi \begin{pmatrix}0&1\\-1&\delta\end{pmatrix}\varphi_1$, где $\delta=-\dfrac{b+b_1}{2|a_1|}$.

Лемма. $\delta=-\operatorname{sign} a_1\left[\dfrac{b+\sqrt{D}}{2|a_1|}\right]$, ~~$b_1=-b-2a_1\delta$~~, где $\operatorname{sign} x=\begin{cases}-1, & \text{если } x<0\\ 0, & \text{если } x=0\\ +1, & \text{если } x>0.\end{cases}$

Мы имеем: $b_1=-b-|2a|\delta$; $\sqrt{D}>-b+2|a_1|\left[\dfrac{b+\sqrt{D}}{2|a_1|}\right]>\sqrt{D}-2|a_1|$ т.к. мы $[y]$ заменяем через $y-1$; т.к. $-b+2|a_1|\left[\dfrac{b+\sqrt{D}}{2|a_1|}\right]\equiv -b \pmod{2|a_1|}$ и заключается в промежутке $\sqrt{D}\ldots\sqrt{D}-2|a_1|$, то это выражение $=b_1$, и δ действительно имеет искомую форму.

Теорема. У каждой приведенной формы есть одна и только одна приведенная ф. эквивалентная соседняя слева. Заметим, что если $\varphi=(a\,b\,a_1)$ — приведенная форма, то и $\psi=(a_1\,b\,a)$ тоже приведенная т. к. a и a_1 удовлетворяют одним и тем же неравенствам.

Пусть привед. форма, соседняя ψ справа, есть $(a\,b'\,a')$, тогда $(a',\,b',\,a)$ есть тоже приведенная форма и в то-же время соседняя к φ слева. Допустим, что $(a''\,b''\,a)$ другая соседняя слева относ. φ эквивалентная приведенная форма. Тогда ψ имело бы справа 2 экв. соседних привед. формы $(a\,b'\,a')$ и $(a\,b''\,a'')$, что противоречит доказанной раньше теореме. Теорема доказана.

Пусть φ_0 приведенная форма; φ_1 приведенная соседняя ей справа, φ_2 соседняя с φ_1 и т. д. Получим ряд эквивал. и приведенных форм $\varphi_0, \varphi_1, \varphi_2, \dots \varphi_\lambda, \dots$ Т. к. общее число приведенных форм конечно, то непременно встретим $\varphi_\lambda = \varphi_{\lambda+\mu}$; т. к. у каждой формы только один левый сосед, то $\varphi_{\lambda-1} = \varphi_{\lambda+\mu-1}$ и т. д.; $\varphi_0=\varphi_\mu$. Берем наименьшее μ, для которого это равенство справедливо; оно непременно четное, т. к. у a и a_1 всегда разные знаки. Пусть в этом ряду $\varphi_{2n}=\varphi_0$. Тогда $\varphi_0, \varphi_1, \dots \varphi_{2n-1}$ суть разные приведенные эквивалентные формы. Наш ряд может и исчерпать все приведенные формы; в противном случае, ~~в противно~~ окажутся другие ряды эквивалентных форм, но число этих рядов всегда конечно; +

Теорема. 2 приведенные формы из разных рядов не могут быть эквивалентные (доказана Гауссом, привед. доказ. – Mertens'a).

Пусть $\varphi=(a,b,c)$ и $\psi=(a'b'c')$ 2 ~~разн~~ приведенные формы разных рядов. Без ограничения общности можем положить $a>0$, $a'>0$ (если бы этого не было, то мы взяли бы вместо формы ея правого соседа). Следовательно, $c<0$, $c'<0$. Допустим, что $\varphi\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\psi$. Получаем уравнения:

$$(1)\quad a'=a\alpha^2+b\alpha\gamma+c\gamma^2$$

$$(2)\quad b'=2a\alpha\beta+b(\alpha\delta+\beta\gamma)+2c\gamma\delta=0$$

$$(3)\quad c'=a\beta^2+b\beta\delta+c\delta^2$$

$$(4)\quad \alpha\delta-\beta\gamma=1$$

Из (1) $\alpha\neq0$, из (3) $\delta\neq0$. Без огранич. общности положим $\alpha>0$ иначе мы ввели бы подстановку $\begin{pmatrix}-\alpha & -\beta\\ -\gamma & -\delta\end{pmatrix}=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$

Из (1) и (2) исключаем a

$$2a'\beta-b'\alpha=b(2\alpha\beta-\alpha^2\delta-\alpha\beta\gamma)+c(2\beta\gamma^2-2\alpha\gamma\delta) \quad \text{или}$$

$$(5)\quad 2a'\beta-b'\alpha=-b\alpha-2c\gamma.$$

Из (2) и (3) исключаем a.

$$b'\beta-2c'\alpha=b(\alpha\beta\delta-\beta^2\gamma-2\alpha\beta\delta)+c(2\beta\gamma\delta-2\alpha\delta^2) \quad \text{или}$$

$$(6)\quad b'\beta-2c'\alpha=-b\beta-2c\delta.$$

I. a) $\beta=0$. Из (2) $b'=b\alpha\delta+2c\gamma\delta$, $\alpha\delta-\beta\gamma=1$, т. е. $\alpha\delta=1$, $\alpha=1$, $\delta=1$, сл. $b'=b+2c\gamma$. Ур. (3) дает $c=c'$; $\gamma=\frac{b'-b}{2c}=\frac{\sqrt{D}-b'}{-2c'}-\frac{\sqrt{D}-b}{-2c}$. Т. к. φ и ψ привед., то обѣ дроби лежат между 0 и 1 $[0 \leq \sqrt{D}-b' < -2c']$; γ = цѣлому числу, сл. $\gamma = 0$. В этом случаѣ $\varphi = \psi$.

в). $\gamma = 0$. Из (2) $b' = 2a\alpha\beta + b\alpha\delta$; опять $\alpha = 1$, $\delta = 1$; $b' = 2a\beta + b$. Из (1) $a' = a$. $\beta = \frac{b'-b}{2a} = \frac{\sqrt{D}-b}{2a} - \frac{\sqrt{D}-b'}{2a'}$; как в предыдущем случаѣ $\beta = 0$, т. е. $\varphi = \psi$.

II. $\beta \neq 0$ и $\gamma \neq 0$. Случай $\beta < 0$ можно свести на случай $\beta > 0$. Пусть $\beta < 0$. Лѣвая часть ур. (5) отрицательна, слѣд. $b\alpha + 2c\gamma > 0$

Умножаем (2) на $2c$

$$2b'c = 4ac\alpha\beta + 2bc(\alpha\delta+\beta\gamma) + 4c^2\gamma\delta;\quad 2b'c + D\alpha\beta = b^2\alpha\beta + 2bc(\alpha\delta+\beta\gamma) + 4c^2\gamma\delta = (b\alpha+2c\gamma)(b\beta+2c\delta)$$

Лѣвая ч. отрицательна ($D>0, \alpha>0, \beta<0$), $b\alpha + 2c\gamma > 0$, слѣд. $b\beta + 2c\delta < 0$; $b\beta + c\delta < 0$. Уравнение (3) даст:

$$(b\beta + c\delta)\delta = c' - a\beta^2;$$ правая часть отриц., слѣд. $\delta > 0$.

Берем обратную ~~[illegible]~~ подстановку: $\psi\begin{pmatrix}\delta & -\beta\\ -\gamma & \alpha\end{pmatrix} = \begin{pmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{pmatrix}\varphi$. В новой подстановкѣ $\beta' > 0$, $\alpha' > 0$, т. е. мы свели к желаемому случаю.

Итак, мы имѣем: $\alpha > 0, \beta > 0, \gamma \neq 0, \delta \neq 0$. В ур. (6) в 1ой части оба члена положительны, слѣд. $-2c\delta > 0$, т. е. $\delta > 0$. Уравнение (4) дает: $\gamma = \frac{\alpha\delta - 1}{\beta} > 0$. Итак, надо рассмотрѣть только случай положительных $\alpha, \beta, \gamma, \delta$.

Берем праваго сосѣда от φ; $\varphi\begin{pmatrix}0 & 1\\ -1 & q\end{pmatrix}\varphi_1$. Мы имѣли $\delta = -\operatorname{sign} a_1 \left[\frac{b+\sqrt{D}}{|2a_1|}\right]$ сл. $q = \left[\frac{b+\sqrt{D}}{-2c}\right]$. Докажем, что тоже число опредѣлится из уравнения.

4?

(7) $\delta = q\beta + r$, где (8) $0 < r \leqq \beta$.

Умножаем (3) на $4c$.

$$4cc' = 4ac\beta^2 + 4bc\beta\delta + 4c^2\delta^2 = (2c\delta + b\beta)^2 - D\beta^2;$$ делим на β^2

$D - \left(2c\frac{\delta}{\beta} + b\right)^2 = -\frac{4cc'}{\beta^2} = \left(\sqrt{D} + 2c\frac{\delta}{\beta} + b\right)\left(\sqrt{D} - 2c\frac{\delta}{\beta} - b\right)$. Вставляем δ из ур. (7)

$\sqrt{D} + 2c\frac{\delta}{\beta} + b = \sqrt{D} + 2c\left(q + \frac{r}{\beta}\right) + b = \sqrt{D} + b + 2qc + \frac{2cr}{\beta}$

$\sqrt{D} - 2c\frac{\delta}{\beta} - b = \sqrt{D} + \frac{b'\beta + 2c'\alpha}{\beta}$ (из ур. (6)) $= \sqrt{D} + b' - 2c'\frac{\alpha}{\beta}$. След.

$\left(\sqrt{D} + b + 2qc + \frac{2cr}{\beta}\right)\left(\sqrt{D} + b' - 2c'\frac{\alpha}{\beta}\right) = -\frac{4cc'}{\beta^2}$; откуда

$$\left(\frac{\sqrt{D}+b}{-2c} - q - \frac{r}{\beta}\right)\left(\frac{\sqrt{D}+b'}{-2c'} + \frac{\alpha}{\beta}\right) = -\frac{1}{\beta^2}; \quad \frac{\sqrt{D}+b}{-2c} - q - \frac{r}{\beta} = -\frac{1}{\beta^2\left(\frac{\sqrt{D}+b'}{-2c'} + \frac{\alpha}{\beta}\right)};$$

$$\frac{\sqrt{D}+b}{-2c} - q = \frac{1}{\beta}\left(r - \frac{1}{\beta\left(\frac{\sqrt{D}+b'}{-2c'} + \frac{\alpha}{\beta}\right)}\right) = \frac{r}{\beta}\left(1 - \frac{1}{\beta r\left(\frac{\sqrt{D}+b'}{-2c'} + \frac{\alpha}{\beta}\right)}\right) \quad (9)$$

$\frac{\sqrt{D}+b'}{-2c'} > 1$ из условия приведенности; $\frac{\alpha}{\beta} > 0$. След. $0 < \frac{\sqrt{D}+b}{-2c} - q < 1$

Требуемое доказано

Итак $\varphi \begin{pmatrix} 0 & 1 \\ -1 & q \end{pmatrix} \varphi_1$, где $q = \left[\frac{\sqrt{D}+b}{-2c}\right] \geqq 1$. Обратно $\varphi_1 \begin{pmatrix} q & -1 \\ 1 & 0 \end{pmatrix} \varphi$;

$\varphi_1 \begin{pmatrix} q & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} q\alpha-\gamma, & q\beta-\delta=-r \\ \alpha & \delta \end{pmatrix}\psi$. Положим $\gamma - q\alpha = \gamma'$, $r = \delta'$;

$\varphi_1 \begin{pmatrix} -\gamma' & -\delta' \\ \alpha & \beta \end{pmatrix}\psi$, где $0 < \delta' \leqq \beta$; из (7) $r < \delta$, сл. $\delta' < \delta$, $\gamma' < \gamma$. Кроме того

$\gamma' \geqq 0$, т.к. $-\beta\gamma' + \alpha\delta' = 1$, $\gamma' = \frac{\alpha\delta' - 1}{\beta} \geqq 0$. Итак, имеем 2 таблицы коэф. подстановок, переводящих φ в ψ и φ_1 в ψ:

$\alpha, \beta, \gamma, \delta$	$0 \leqq \gamma' < \gamma$
$-\gamma', -\delta', \alpha, \beta$.	$0 < \delta' < \delta$.

Ищем правого соседа φ_1; $\varphi_1 \begin{pmatrix} 0 & 1 \\ -1 & Q \end{pmatrix} \varphi_2$, $\beta = Q\delta' + R$, $0 \leqq R \leqq \delta' - 1$.

При этом (докажем, что) $-Q=-\operatorname{sign} c_1\left[\frac{b_1+\sqrt{D}}{|2c_1|}\right]$ или $Q=\left[\frac{b_1+\sqrt{D}}{2c_1}\right]$; и a, b, c c, c_1

В формуле (9) делаем замену букв: $q \ldots -Q$, $r \ldots R$. Получаем:

$$\frac{\sqrt{D}+b_1}{-2c_1}+Q=\frac{1}{-\delta'}\left(R-\frac{1}{-\delta'\left(\frac{\sqrt{D}+b'}{-2c'}+\frac{\gamma'}{\delta'}\right)}\right) \text{ или } \frac{\sqrt{D}+b_1}{2c_1}-Q=\frac{1}{\delta'}\left(R+\frac{1}{\delta'\left(\frac{\sqrt{D}+b'}{-2c'}+\frac{\gamma'}{\delta'}\right)}\right)$$

Имеем: $\delta'>1$, $\frac{\sqrt{D}+b'}{-2c'}>1$, $\frac{\gamma'}{\delta'}\geqq 0$; значит $\frac{\sqrt{D}+b_1}{2c_1}-Q<1$; $Q\geqq 1$ из условий приведенности. Мы имеем:

$\varphi_1\begin{pmatrix}0&-1\\1&Q\end{pmatrix}\varphi_2$ или $\varphi_2\begin{pmatrix}Q&1\\-1&0\end{pmatrix}\varphi_1$ или $\varphi_2\begin{pmatrix}Q&1\\-1&0\end{pmatrix}\begin{pmatrix}-\gamma'&-\delta'\\\alpha&\beta\end{pmatrix}=\begin{pmatrix}-Q\gamma'+\alpha & -Q\delta'+\beta\\\gamma'&\delta'\end{pmatrix}=$
$=\begin{pmatrix}\alpha'&\beta'\\\gamma'&\delta'\end{pmatrix}\psi$, где $\alpha'=-Q\gamma'+\alpha$, $\beta'=-Q\delta'+\beta=R$. Кроме того

$0\leqq\gamma'<\gamma$, $0<\delta'<\delta$; $\beta'\leqq\beta$, сл. $0\leqq\beta'=R\leqq\delta'-1\leqq\beta-1$, т. е. $\beta'<\beta$.

Если $\beta'=0$ или $\gamma'=0$, то мы сведем дело к 1-му случаю*); φ_2 и ψ тождественны, т. е. φ и ψ не могут принадлежать к разным рядам.

2-ой случай $\beta'\neq 0$, $\gamma'\neq 0$. Тогда $\beta'>0$, $\gamma'>0$; $\alpha'=\frac{1+\beta'\gamma'}{\delta'}>0$; $\alpha'=-Q\gamma'+\alpha$, сл. $\alpha'<\alpha$.

Итак $\alpha'<\alpha$, $\beta'<\beta$, $\gamma'<\gamma$, $\delta'<\delta$ и все коэф. положительны. Применяя тот же процесс еще раз, мы определим все положительные α'', β'', γ'', δ'' соотв. меньшие чем α', β', γ', δ'. Т. к. этот процесс не может продолжаться бесконечно, то когда наступит 1-ый случай β или $\gamma=0$. Тогда $\varphi_{2n}=\psi$, т. е. ψ всегда окажется в одном ряду с φ. Теорема доказана.

---

*) Из урав. $\alpha'\delta'-\beta'\gamma'=1$ им. $\alpha'\delta'=1$, но $\delta'>0$, сл. $\alpha'=1$, $\delta'=1$; имеем $\varphi_2=\psi$, но $\varphi_2\sim\varphi$, сл. $\psi\sim\varphi$

Глава 8.

О проблемѣ Waring'а.

Waring высказал предположение, что каждое число может быть представлено в видѣ конечнаго числа $n^{\text{ых}}$ степеней цѣлых чисел. Для $2^{\text{х}}$ степеней впервые была доказана Lagrange'м слѣдующая теорема:

Каждое число может быть представлено в видѣ суммы 4 квадратов цѣлых чисел (в числѣ этих чисел могут быть нули).

<u>1 часть доказ.</u> Каждое простое число вида $p = 4n+1$ может быть разложено на сумму $2^{\text{х}}$ квадратов (и притом единственным образом).

<u>$1^{\text{е}}$ доказ.</u> $p = 4n+1$, слѣд. $\left(\frac{-1}{p}\right) = 1$. Сравнение $1+u^2 \equiv 0 \pmod p$ разрѣшимо; выберем u так, чтобы $0 \leqq u \leqq p-1$. Тогда $1+u^2 = Mp$; ~~это~~ $Mp>0$, сл. $M>0$; $Mp \leqq 1+(p-1)^2 = p^2-2p+2 < p^2$, слѣд. $1 \leqq M < p$. Итак, существует кратное p, $< p^2$ и разложимое на сумму $2^{\text{х}}$ квадратов. Если $M = 1$, положение доказано.

Допустим, что p неразложимо на сумму $2^{\text{х}}$ квадратов, и M наименьшее число такое, что $Mp = \square + \square$; $1 < M < p$.

$v^2+w^2 = Mp$. Берем абсолютно наименьшие вычеты от v и $w \pmod M$

$v \equiv v_0 \pmod M$, $|v_0| \leqq \frac{M}{2}$; $w \equiv w_0 \pmod M$, $|w_0| \leqq \frac{M}{2}$.

$v_0^2+w_0^2 \equiv v^2+w^2 \pmod M$; $v_0^2+w_0^2 = M.N$. Если бы $N = 0$, то $v_0 = 0$, $w_0 = 0$

$9 = 109$ $\qquad 10x + y =$

$49 = 436$ $\qquad 100x + 10y + z =$

$49 + 5 = 441$ $\qquad 97x + 7y = 2z$

$\sqrt{441} = 21$ $\qquad 100x + 10y + z =$

$p + 2 = 21$ $\qquad (100-n)x + (10-n)y = (n-1)z$

$p = 19$ $\qquad \left(\frac{100-n}{n-1}\right)x + \left(\frac{10-n}{n-1}\right)y = z$

$3p = 57$ $\qquad (100-n)x \quad (n-1)\cdot z$

$3p + 1 = 58$ $\qquad 100 - n < (n-1)\cdot 9$

$9n - 9$

$\frac{1}{2}(\;) = 29$ $\qquad 109 < 10n$

$n > 10{,}9$

$p < 29$ $\qquad 90x +$

$100x + 10y + z$

$x + y + z$

$90x + 99x + 9y + 9z - 9z$

$x + y + z$

$90x - 9z$

$x + y + z$

$10x - z > x + y + z$

10-1
10-2
10-3
10-4
10-5

$10x - z > x + y + z$

$9x > 2z$

$x + y + z$

$x + y + z$

$x + y + (z)$

$n \leq v - 3.1\ldots \leq n$

$v \geq 10. + 3. \ldots \geq n$

$u \leq 10 \cdot 5^{3v} + 3 \cdot 1250^{\frac{2}{3}} 5^{2v}$

$v \leq u + 3 \cdot 1250^{\frac{2}{3}} \cdot 5^{2v}$

$v - u \leq 3 \cdot 12 \cdot 50^{\frac{2}{3}} 5^{2v}$

показали,

тавлено ква

$$10 \cdot 5^{3\nu} + 6 \cdot 1250^{\frac{2}{3}} \cdot 5^{2\nu}$$

$$\cancel{2 \cdot 5^{3\nu+1}}$$

$5^3 = 125$ $\quad 5^6 =$ $\quad 5^3 = 125$

$5 \cdot 5 \cdot 5 \cdot 5$ $\quad 5 \quad 125$

$10 \cdot 5^{3\nu} \leq$

$a + bi \quad c + di$

$-c - di \quad a - bi$

$\alpha\delta - \beta\beta + (\alpha\beta + \alpha\beta)i$

$(n-1)(n+1)(n+2)$

$n^3 - n$

$v_0 = 0,$

$M|v$, $M|w$, сл. $M^2 | v^2+w^2 = Mp$, т.е. $M|p$; абсурд, т.к. p простое.
След. $N \geq 1$; $MN \leq \frac{M^2}{4}+\frac{M^2}{4}=\frac{M^2}{2}$, $N \leq \frac{M}{2}$. Итак $1 \leq N < M$.
Воспользуемся очевидным тождеством:

$$(a^2+b^2)(\alpha^2+\beta^2)=(a\alpha+b\beta)^2+(a\beta-b\alpha)^2.$$

$$(v^2+w^2)(v_0^2+w_0^2) = (vv_0+ww_0)^2+(vw_0-wv_0)^2 = M^2pN.$$

Каждая скобка делится на M; в с.д.

$$vv_0+ww_0 \equiv v^2+w^2 \equiv 0 \pmod M; \quad vw_0-wv_0 \equiv vw-wv \equiv 0 \pmod M;$$

Обозначим: $\frac{vv_0+ww_0}{M}=v_1$; $\frac{vw_0-wv_0}{M}=w_1$, где v_1 и w_1 — цел. числа.
Имеем:

$v_1^2+w_1^2=Np$; т.е. Mp не есть наименьшее из кратных p, разлагающееся на сумму двух квадратов. Мы пришли к противоречию, предположив, что $p \neq \square+\square$. Положение доказано.

2ое доказательство.

Лемма. Число классов форм с дискриминантом $D=-4$ есть 1.
Для приведенной формы мы имеем:

$|b| \leq \sqrt{\frac{\Delta}{3}}=\sqrt{\frac{4}{3}}$; $a \leq \sqrt{\frac{\Delta}{3}}$; далее $b \equiv D \pmod 2$, след. $b=0$.
$-4ac=-4$, $ac=1$; $a=1$, $c=1$. Итак, единственная приведенная форма с $D=-4$ есть x^2+y^2.

Докажем, что простое число $p=4n+1$ может быть собственно представлено квадратичной формой с $D=-4$.
Мы видели, что необходимое условие, чтобы p могло быть представлено

формой (a,b,c) дискр. D есть: D есть квадрат. вычет $(\bmod 4k)$.
[~~Докажем~~ Легко показать, что для нашего случая это условие и достаточно]

Нам надо доказать, что $p = x^2+y^2$ или, что по предыдущему тоже, p может быть представлено формой с $D=-4$.
Наше условие выполняется, т.к. -4 есть квадратичный вычет $\bmod 4p$.
$u^2 \equiv -1 \pmod p$; $(2u)^2 \equiv -4 \pmod{4p}$.
Т.к. p представляется формой $(1,0,1)$, то $(1,0,1) \sim (p,l,m)$;
$l^2 \equiv D \pmod{4p}$. Докажем, что в нашем случае это сравнение имеет только 2 корня $(\bmod 2p)$. Рассмотрим сравнение:
$x^2 \equiv -4 \pmod{4p}$; сделаем замену: $x = 2u$;
$4u^2 \equiv -4 \pmod{4p}$ или $u^2 \equiv -1 \pmod p$. u имеет только 2 корня $\bmod p$, т.е. x имеет только 2 корня $\bmod 2p$, пусть это будут $2v, 2w$.

Перейдем к общей теореме: каждое число может быть представлено в виде суммы 4 квадратов. Воспользуемся тождеством.

$(a^2+b^2+c^2+d^2)(\alpha^2+\beta^2+\gamma^2+\delta^2) =$
$= (a\alpha+b\beta+c\gamma+d\delta)^2+(a\beta-b\alpha+c\delta-d\gamma)^2+(a\gamma-c\alpha+d\beta-b\delta)^2+(a\delta-d\alpha+b\gamma-c\beta)^2$.

Оно показывает, что, если теорема верна для 2^x чисел, то она справедлива и для их произведения. Т. обр. нам достаточно показать ее справедливость для всех простых чисел.

Для 2 она очевидна, т. к. $2 = 1^2+1^2$, для простых чисел типа $4n+1$ доказана,
остается доказать для простых чисел типа $4n+3$.

<u>2ая часть.</u> $p = 4n+3$; $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{p-1}{p}\right) = -1$; $\left(\frac{1}{p}\right) = 1$. Пишем послед. чисел
$1, 2, 3, \ldots p-2, p-1$; 1ое есть квадр. вычет, последнее невычет $(\mathrm{mod}\ p)$.
Следов. найдется такое r, что $\left(\frac{r}{p}\right) = 1$, $\left(\frac{r+1}{p}\right) = -1$; $1 \leqq r \leqq p-1$.
Умножая последний символ на $\left(\frac{-1}{p}\right)$, имеем $\left(\frac{-r-1}{p}\right) = 1$.
$t^2 \equiv r\ (\mathrm{mod}\ p)$; $s^2 \equiv -r-1\ (\mathrm{mod}\ p)$. Исключаем r;
$1+t^2+s^2 \equiv 0\ (\mathrm{mod}\ p)$. Значит, некоторое число, кратное p, есть
сумма 3 квадратов. ~~Пусть~~ значит существует M ~~наименьшее число~~ такое, что
$$Mp = x^2+y^2+z^2+u^2,\quad 1 \leqq M.$$
Берем для t и s значения $0 < t < \frac{p}{2}$, $0 < s < \frac{p}{2}$. Тогда $Mp < \frac{p^2}{4}+\frac{p^2}{4}+\frac{p^2}{4} = \frac{3p^2}{4}$
$M < \frac{3}{4}p$. Итак $1 \leqq M < p$. Если $M = 1$, теорема доказана, если же $\neq 1$, то берем наименьшее M так, чтобы $Mp = \sum_4 \square$
$1 < M < p$. Берем наименьшие абс. вычеты $(\mathrm{mod}\ M)$ от x, y, z, u.
$x \equiv x_0$, $y \equiv y_0$, $z \equiv z_0$, $u \equiv u_0\ (\mathrm{mod}\ M)$; $|x_0|, |y_0|, |z_0|, |u_0| \leqq \frac{M}{2}$.
$x_0^2+y_0^2+z_0^2+u_0^2 = MN$; если $N = 0$, то $x_0 = y_0 = z_0 = u_0 = 0$, $M \mid x, y, z, u$
$M^2 \mid Mp$, $M \mid p$, — абсурд. Значит $1 \leqq N$.
$MN \leqq \frac{M^2}{4}+\frac{M^2}{4}+\frac{M^2}{4}+\frac{M^2}{4} = M^2$; $N \leqq M$. Положим, что $N = M$.
Тогда $x \equiv \frac{M}{2}\ (\mathrm{mod}\ M)$, $y \equiv \frac{M}{2}$, $z \equiv \frac{M}{2}$, $u \equiv \frac{M}{2}\ (\mathrm{mod}\ M)$; $\frac{M}{2} \mid x, y, z, u$;
$\frac{M^2}{4} \mid x^2, y^2, z^2, u^2$, следов. $\frac{M^2}{4} \mid Mp$; $M \mid 4p$; т. к. p простое, то $M \mid 4$.
1) $M = 4$; $4p = x^2+\ldots+u^2$, где x, y, z, u — четные числа; $p = \left(\frac{x}{2}\right)^2+\left(\frac{y}{2}\right)^2+\left(\frac{z}{2}\right)^2+\left(\frac{u}{2}\right)^2$. Теор. док. для этого случая.

2) $M=2$, x, y, z, u — нечетные; $2p = x^2+y^2+z^2+u^2 \equiv 4 \pmod 8$ абсурд.

Остается 3) случай $1 \le N < M$. Перемножаем Σx_0^2 и Σx^2; в левой части, по доказанному, будет сумма 4 квадратов

$$x_1^2+y_1^2+z_1^2+u_1^2 = M^2 pN;$$ докажем, что $M \mid x_1, y_1, z_1, u_1$. В с.

$x_1 = xx_0+yy_0+zz_0+uu_0 \equiv \Sigma x^2 \equiv 0 \pmod M$; $y_1 = xy_0 - yx_0 + zu_0 - uz_0 \equiv xy - xy + zu - zu \equiv 0\ (M)$;

точно так же $z_1 \equiv 0 \pmod M$ и $u_1 \equiv 0 \pmod M$; Обозначим:

$\frac{x_1}{M} = x_2$, $\frac{y_1}{M} = y_2$, $\frac{z_1}{M} = z_2$, $\frac{u_1}{M} = u_2$. Имеем:

$$x_2^2+y_2^2+z_2^2+u_2^2 = Np,$$ т. е. M не наименьшее число.

Теорема о разложении на сумму квадратов доказана (Lagrange)

Теорема. Всякое число может быть представлено в виде суммы 53 четвертых степеней (Liouville).

Исходим из тождества:

$(x+y)^4+(x-y)^4 = 2x^4+12x^2y^2+2y^2$. Составляя такие выражения для любой пары из чисел x, y, z, u и складывая, получим:

$$(x+y)^4+(x-y)^4+(x+z)^4+(x-z)^4+(x+u)^4+(x-u)^4+(y+z)^4+(y-z)^4+(y+u)^4+(y-u)^4+(z+u)^4+(z-u)^4 =$$

$$= 6x^4+6y^4+6z^4+6u^4+12x^2y^2+12x^2z^2+\ldots = 6(x^2+y^2+z^2+u^2)^2.$$

Это тождество показывает, что $6(x^2+y^2+z^2+u^2)^2 = B_{12}$

(сумма 12 биквадратов)

или, т. к. по теореме Lagrange'а в скобках стоит произвольное число, $6n^2 = B_{12}$. Возьмем любое число формы $6m$; по теор. Lagrange'а

$$6m = 6(m_1^2+m_2^2+m_3^2+m_4^2) = B_{48}.$$

Т. к. произвольное число $z = 6m + \{0, 1, 2, 3, 4$ или 5, то $z = B_{53}$, что и требовалось доказать.

[Число 53 дано Liouville'ем в 1859 г., Realis в 1878 дал $z = B_{47}$, Lucas (1878) ... 41, Fleck (1906) ... 39, Landau (1907) ... 38, Wieferich (1908) B_{37}. Кроме того, Landau показал, что для представления бесконечного множества чисел суммы 15 четвертых степеней недостаточно.

Теорема. Начиная с известного предела, каждое число есть сумма 11 кубов. (Wieferich).

Положим $x \geqq y \geqq 0$; пишем тождество:

$$(x+y)^3+(x-y)^3 = 2x^3+6xy^2 = x(2x^2+6y^2).$$ Берем $x \geqq \left\{\begin{matrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{matrix}\right\} \geqq 0$

Составляем 4 аналогичных выражения и складываем:

$$\begin{aligned}
&(x+y_1)^3+(x-y_1)^3+ \\
&(x+y_2)^3+(x-y_2)^3+ \\
&(x+y_3)^3+(x-y_3)^3+ \\
&(x+y_4)^3+(x-y_4)^3 = x\left(8x^2+6(y_1^2+y_2^2+y_3^2+y_4^2)\right).
\end{aligned}$$

Т. к. $y_1^2+y_2^2+y_3^2+y_4^2=$ произвольному числу n, то все числа вида

$$x(8x^2+6n)=K_8 \text{ (сумма 8 кубов), если } 0\leqq 6n\leqq 6x^2,$$

$y_i^2\leqq n\leqq x^2$

Пусть $z>0$ данное целое число*); ~~удовлетворяющее~~ оно удовлетворяет неравенству $125^\nu<\frac{z}{10}\leqq 125^{\nu+1}$; ~~где~~ пусть $\nu\geqq 0$. Отсюда следует $z>10$. Иначе

$$10.5^{3\nu}<z\leqq 1250.5^{3\nu}.$$

Пишем ряд чисел: z, $z-1^3$, $z-2^3$, ... $z-\alpha^3$ ..., пока эти числа $\geqq 0$. По крайней мере 2 первых из них положительны и удовлетворяют неравенству: они $\geqq 10.5^{3\nu}$. Все α найдутся из неравенства $z-\alpha^3\geqq 0$, $\alpha\leqq\sqrt[3]{z}$.

Вычислим разность 2х последовательных чисел нашего ряда.

$$\cancel{z-\alpha^3-(z-(\alpha-1)^3)}\ \underset{(u,v)}{z-(\alpha-1)^3-(z-\alpha^3)}=3\alpha^2-3\alpha+1\underset{\#}{\leqq}3\alpha^2\leqq 3.z^{2/3}\leqq 3.1250^{2/3}.5^{2\nu}.$$

Берем 2 наши числа $\geqq 10.5^{3\nu}$; их разности $<3.1250^{2/3}.5^{2\nu}$.

$10.5^{3\nu}\leqq u<v$; отсюда $v\leqq 10.5^{3\nu}+c.5^{2\nu}$, где $c=6.1250^{2/3}$.

Если ν достаточно велико, то $10.5^{3\nu}\leqq u<v<14.5^{3\nu}$; для этого необх. $c.5^{2\nu}<4.5^{3\nu}$, а этому неравенству всегда можно удовлетворить некоторым значением ν $(\nu=4)$ и всеми большими его.

Если z достаточно велик, то существуют значения $\alpha>0$ такие, что

$$10.5^{3\nu}\leqq z-\alpha^3<z-(\alpha-1)^3\underset{\#}{\leqq}14.5^{3\nu}.$$

Из чисел $z-\alpha^3$ и $z-(\alpha-1)^3$ по крайней мере одно не делится на 5.

*) z больше некоторого опред. числа, которое определим ниже

В с.д., допустив обратное, имеем: $z-\alpha^3\equiv 0 \pmod 5$, $z-(\alpha-1)^3\equiv 0 \pmod 5$
$3\alpha^2-3\alpha+1\equiv 0$ или $36\alpha^2-36\alpha+12\equiv 0$ или $(6\alpha-3)^2+3\equiv 0 \pmod 5$,
а это значило бы $\left(\frac{-3}{5}\right)=1$, ~~тогда~~ что неверно.

Итак, мы доказали $10.5^{3\nu}\leqq z-\alpha^3<14.5^{3\nu}$, причем $(z-\alpha^3, 5)=1$.

(~~Лемма.~~ Введем новое понятие: если $x^3\equiv c \pmod m$, то c называется кубическим вычетом $(\mathrm{mod}\ m)$. Докажем следующую лемму: Каждое число, взаимно простое с m, есть кубический вычет $(\mathrm{mod}\ m)$, если при этом m удовлетворяет условию $(3, \varphi(m))=1$.

(т.к. $\varphi(m)=\prod p^{\alpha-1}(p-1)$, то в m не должен входить ни один простой множитель формы $3n+1$, а 3 может войти только 1 раз).

Док. Пусть $a_1, a_2, \dots a_{\varphi(m)}$ есть система взаимно простых с m вычетов $(\mathrm{mod}\ m)$; тогда числа $a_1^3, a_2^3, \dots a_{\varphi(m)}^3$ будут тоже взаимно простыми с m; докажем, что между собой они несравнимы $(\mathrm{mod}\ m)$. Допустив $a^3\equiv b^3 \pmod m$; $(a, m)=1$, $(b, m)=1$, мы получили бы $a\equiv b \pmod m$,*) а это противоречит условию. Значит $a_1^3, a_2^3, \dots a_{\varphi(m)}^3$ тоже представляют полную систему взаимно простых вычетов.

*) Диофантовское уравнение $3x-\varphi(m).y=1$ разрешимо в целых и положит. числах. Берем одну пару решений (x, y), возводим предполагаемое сравнение $a^3\equiv b^3$ в степень x; $a^{3x}\equiv b^{3x}$; или:

$$a^{1+\varphi(m).y}\equiv b^{1+\varphi(m).y}; \quad \text{т.к. } a^{\varphi(m)}\equiv 1,\ b^{\varphi(m)}\equiv 1, \text{ то}$$

$a\equiv b \pmod m$, что и треб. доказать.

Отсюда следует, что при данном условии всякое взаимно простое с m число есть кубический вычет (mod m.)

Возвращаемся к теореме. Применим доказанную лемму к $m = 5^\nu$. Сравнение $z - \alpha^3 \equiv \beta^3 \pmod{5^\nu}$, ~~где~~ $\cancel{0 \leq \beta \leq 5^\nu}$ по доказанному, разрешимо относительно β; ~~определим~~ возьмем значение β, удовлетворяющее неравенству: $0 \leq \beta < 5^\nu$.

Тогда $z - \alpha^3 - \beta^3$ будет делиться на 5^ν; положим

$z - \alpha^3 - \beta^3 = M \cdot 5^\nu < 14 \cdot 5^{3\nu}$. Имеем неравенство:

$$9 \cdot 5^{2\nu} < M < 14 \cdot 5^{2\nu}, \text{ или}$$

$$5^{2\nu} < M - 8 \cdot 5^{2\nu} = M_1 < 6 \cdot 5^{2\nu}.$$

Мы доказали сначала, что число вида $x(8x^2+6n) = K_8$, если $x \geq 0$, $0 \leq 6n \leq 6x^2$. Теперь мы видим, что всякое достаточно большое z можно представить так:

$$z = \alpha^3 + \beta^3 + 5^\nu(8 \cdot 5^{2\nu} + M_1).$$ Рассмотрим случаи:

где $x = 5^\nu$

1) $6 \mid M_1$. Положим тогда $M_1 = 6n$; $0 < 6n < 6x^2$, Следовательно 3-е слагаемое $= K_8$, $z = K_{10}$

2) $6 \nmid M_1$; ~~a) $3|\nu$~~ Сравнение; разрешимо $M_1 - \gamma^3 \equiv 0 \pmod 6$, где $\gamma = 1, 2, 3, 4, 5$.

a) $3|\nu$. $z = \alpha^3 + \beta^3 + 5^\nu(8 \cdot 5^{2\nu} + (M_1 - \gamma^3)) + 5^\nu \cdot \gamma^3 = K_{11}$.

b) $\nu \equiv 1 \pmod 3$. Сравнение $M_1 - 25\gamma \equiv 0 \pmod 6$ разрешимо, значит разрешимо и сравнение $M_1 - 25\gamma^3 \equiv 0 \pmod 6$, где $\gamma = 1, 2, 3, 4, 5$

$$z = \alpha^3 + \beta^3 + 5^\nu(8 \cdot 5^{2\nu} + (M_1 - 25\gamma^3)) + 5^\nu \cdot 25\gamma^3 = K_{11}.$$

c) $\nu \equiv 2 \pmod 3$. Сравнение $M_1 - 5y^3 \equiv 0 \pmod 6$ разрешимо ($y = 1, 2, 3, 4, 5$)

$$z = \alpha^3 + \beta^3 + 5^\nu (8.5^{2\nu} + (M_1 - 5y^3)) + 5.5^\nu y^3 = K_{11}.$$

Теорема доказана.

Теорема. Каждое число может быть представлено в виде суммы конечного числа 6 степеней.

Исходим из тождества:

$$(a+b+c)^6 + (-a+b+c)^6 + (a-b+c)^6 + (a+b-c)^6 + (a+b+d)^6 + (-a+b+d)^6 + (a-b+d)^6 + (a+b-d)^6 +$$
$$+ (a+c+d)^6 + (-a+c+d)^6 + (a-c+d)^6 + (a+c-d)^6 + (b+c+d)^6 + (-b+c+d)^6 + (b-c+d)^6 + (b+c-d)^6 +$$
$$+ 2(a+b)^6 + 2(a-b)^6 + 2(a+c)^6 + 2(a-c)^6 + 2(a+d)^6 + 2(a-d)^6 + 2(b+c)^6 + 2(b-c)^6 +$$
$$+ 2(b+d)^6 + 2(b-d)^6 + 2(c+d) + 2(c-d)^6 +$$
$$+ 36a^6 + 36b^6 + 36c^6 + 36d^6 \qquad = 60(a^2+b^2+c^2+d^2)^3.$$

Чтобы проверить это тождество, замечаем, что оно симметрично относительно всех 4 букв; достаточно сравнить в обеих частях коэффициенты при a^6; a^4b^2, $a^2b^2c^2$.

При a^6: $12 + 2.6 + 36 = 60$: верно.

при a^4b^2: $8.15 + 2.2.15 = 180 = 60.3$ верно

при $a^2b^2c^2$: $4.\frac{6!}{2!2!2!} = 360 = 60.\frac{3!}{1!1!1!} = 360$ верно.

В левой части стоит сумма $16 + 2.12 + 4.36 = 184$ шестых степеней.

Тождество показывает, что всякое число вида $60n^3 = P_{184}$

Если число имеет вид $60m$, то предыдущему, оно равно

$60(n_1^3+n_2^3+\ldots+n_N^3)$, где N во всяком случаѣ конечное число.
Значитъ, $60m = P_{184N}$; т. к. любое число
$z = 60m + r$ $(r=0,1,2,\ldots 59)$, то имѣем
$z = P_{184N+59}$. Теорема доказана.

Теорема Гильберта (Hilbert).

Всякое число может быть представлено въ видѣ суммы N
$n^{ых}$ степеней цѣлыхъ полож. чисел, гдѣ N зависит только отъ n.

Докажем сначала слѣдующее тождество:

$$(x_1^2+x_2^2+x_3^2+x_4^2+x_5^2)^m = \sum \rho_k (a_{1k}x_1+a_{2k}x_2+a_{3k}x_3+a_{4k}x_4+a_{5k}x_5)^{2m},$$

гдѣ всѣ a – цѣлыя, ρ – положительныя раціональныя числа

(Проводимое доказ. этого тождества принадлежит Hausdorff'у).

Берем функцію e^{-x^2} и пишем выраженія для послѣдовательных производных:

$$D\,e^{-x^2} = -2x\,e^{-x^2}$$

$$D^2 e^{-x^2} = (-2+4x^2)e^{-x^2} \quad \text{и т. д. Вообще}$$

$$D^m e^{-x^2} = e^{-x^2}(-2)^m \cdot f_m(x),$$

гдѣ $f_m(x)$ – многочлен $m^{ой}$ степени. ~~с цѣлыми коэффиціентами~~

Мы имѣем $f_1(x) = x$; докажем слѣдующую рекуррентную формулу:

$$f_{m+1}(x) = x \cdot f_m(x) - \tfrac{1}{2} f_m'(x)$$

Дифференцируем, получаем:
(выраженіе $D^m e^{-x^2} = e^{-x^2}(-2)^m \cdot f_m(x)$)

$$D^{m+1}e^{-x^2} = e^{-x^2}\left((-2x)(-2)^m f_m + (-2)^m f_m'\right) = e^{-x^2}(-2)^{m+1} f_{m+1},$$

откуда $f_{m+1} = x f_m - \frac{1}{2} f_m'$. Формула доказана.

Общее выражение для f_m таково:

$$f_m = x^m - \binom{m}{2}\frac{1}{2} x^{m-2} + \binom{m}{4}\frac{1}{2}\cdot\frac{3}{2} x^{m-4} - \binom{m}{6}\frac{1}{2}\cdot\frac{3}{2}\cdot\frac{5}{2} x^{m-6} + \dots + (-1)^k\binom{m}{2k}\frac{1}{2}\cdot\frac{3}{2}\cdots\frac{2k-1}{2}x^{m-2k}+\dots$$

Эта формула справедлива для $m=1$. Допустив её справедливость для m, докажем, что она верна для $m+1$.

$$f_{m+1} = x f_m - \frac{1}{2} f_m' = x^{m+1} + x^{m-1}\left(-\frac{m^2-m}{4}-\frac{m}{2}\right)+\dots$$
$$+ (-1)^k x^{m+1-2k}\left(\binom{m}{2k}\frac{1}{2}\cdot\frac{3}{2}\cdots\frac{2k-1}{2} + \frac{1}{2}(m+2-2k)\binom{m}{2k-2}\frac{1}{2}\cdot\frac{3}{2}\cdots\frac{2k-3}{2}\right)+\dots$$

Преобразуем выражение коэф. при общем члене*) он =

$$\frac{m(m-1)\dots(m-2k+1)}{2k!}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdots\frac{2k-1}{2} + \frac{m(m-1)\dots(m-2k+3)(m-2k+2)}{(2k-2)!}\frac{1}{2}\cdot\frac{3}{2}\cdots\frac{2k-3}{2} =$$

$$= \frac{m(m-1)\dots(m-2k+2)}{2k!}\left((m-2k+1)\frac{1}{2}\cdot\frac{3}{2}\cdots\frac{2k-1}{2} + \frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdots\frac{2k-3}{2}(2k-1)2k\right) =$$

$$= \frac{(m+1)m\dots(m-2k+2)}{2k!}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdots\frac{2k-1}{2}(m-2k+1+2k) = \binom{m+1}{2k}\frac{1}{2}\cdot\frac{3}{2}\cdots\frac{2k-1}{2}.$$

Справедливость формулы т. обр. доказана.

*Пусть теперь m пол. целое число ≥ 1; $0 \leq n \leq m-1$, где n целое число.

Тогда $\int_{-\infty}^{\infty} e^{-x^2} f_m(x)x^n\,dx = 0$. (Заметим, что это равенство очевидно, если одно из чисел m, n нечетное).

$$\int_{-\infty}^{\infty} e^{-x^2}f_m(x)x^n\,dx = \frac{1}{(-2)^m}\int_{-\infty}^{+\infty} D^m(e^{-x^2})x^n\,dx;$$ Заметим, что при $m=1$ $(n=0)$

---

*) Коэф. при 2-м члене $= \frac{-m^2+m-2m}{4} = -\binom{m+1}{2}\cdot\frac{1}{2}$

$$\int_{-\infty}^{\infty} \frac{d}{dx} e^{-x^2} dx = \left[e^{-x^2} \right]_{-\infty}^{\infty} = 0;$$

$$\int_{-\infty}^{+\infty} x^n D^m e^{-x^2} dx = \left[x^n D^{m-1} \right]_{-\infty}^{+\infty} - n \int_{-\infty}^{\infty} x^{n-1} D^{m-1} dx = \left[x^n D^{m-1} \right] - n \left(\left[x^{n-1} D^{m-2} \right]_{-\infty}^{\infty} - (n-1) \int_{-\infty} x^{n-2} D^{m-2} dx \right) =$$

$$= \ldots = \left[x^n D^{m-1} \right]_{-\infty}^{\infty} - n \left[x^{n-1} D^{m-2} \right]_{-\infty}^{\infty} + n(n-1) \left[x^{n-2} D^{m-3} \right]_{-\infty}^{\infty} - \ldots + (-1)^n n(n-1) \ldots 1 . \underbrace{\int_{-\infty}^{\infty} x^0 D^{m-n} dx}_{\left[D^{m-n-1} \right]_{-\infty}^{+\infty}};$$

и мы видим, что при подстановкѣ всѣ члены обращаются в 0. Формула доказана; при этом $n = 0, 1, \ldots m-1$.

Умножая соотвѣтствующія равенства на $a_0, a_1, \ldots a_{m-1}$ и складывая, имѣем:

$$\int_{-\infty}^{\infty} e^{-x^2} f_m(x) (a_0 + a_1 x + \ldots + a_{m-1} x^{m-1}) dx = 0 \text{ или } \int_{-\infty} e^{-x^2} f_m g_{m-1} dx = 0,$$

гдѣ g_{m-1} — любой многочлен $m-1^{\text{ой}}$ степени.

Уравненіе $f_m(x) = 0$ имѣет всѣ корни различные и действительные. Это вѣрно для $m = 1$. Допустим справедливость этого положенія для m и докажем для $m+1$.

Пусть корни f_m суть $\beta_1, \beta_2, \ldots, \beta_m$ — в возрастающем порядкѣ; знаки f'_m в соотвѣтствующих точках чередуются, а именно

$$\text{sign } f'_m(\beta_k) = (-1)^{m-k}.$$

$$f_{m+1}(\beta_k) = 0 - \tfrac{1}{2} f'_m(\beta_k); \quad \text{sign } f_{m+1}(\beta_k) = (-1)^{m+1-k}$$

Кромѣ того, в точкѣ $-\infty$ f_{m+1} имѣет знак $(-1)^{m+1}$, а в точкѣ $+\infty$ $(-1)^0 = +1$.

Итак $f_{m+1}(x)$ имѣет в $m+2$ точках $-\infty, \beta_1, \ldots \beta_m, +\infty$ разные чередующіеся знаки; слѣд. между каждыми $2^{\text{мя}}$ должен быть хоть один корень, т. е.

число промеж. $m+1$, что f_{m+1} имеет $m+1$ различных действ. корней. Теорема доказ.

~~Итак~~ Обозначим $\int_{-\infty}^{\infty} e^{-x^2}dx = \sqrt{\pi} = \gamma$.

Если n целое число ≥ 0, то $\frac{1}{\gamma}\int_{-\infty}^{\infty} e^{-\alpha^2}\alpha^n d\alpha = l_n$

докажем, что все l_n рациональны. $l_0 = 1$.

$l_1 = l_3 = l_5 = \dots = 0$, т.к. под интегралом нечетная функция.

Для доказательства в случае четного n докажем рекуррентную формулу: $l_n = \frac{n-1}{2} l_{n-2}$ $(n \geq 2)$.

$$\int_{-\infty}^{\infty} e^{-\alpha^2}\alpha^n d\alpha = \int_{-\infty}^{\infty} -2\alpha e^{-\alpha^2}\cdot\frac{-\alpha^{n-1}}{2}d\alpha = \left[e^{-\alpha^2}\left(-\frac{\alpha^{n-1}}{2}\right)\right]_{-\infty}^{\infty} + \frac{n-1}{2}\int_{-\infty}^{\infty} e^{-\alpha^2}\alpha^{n-2}d\alpha,$$

$l_n\gamma = \frac{n-1}{2}l_{n-2}\cdot\gamma$, т.е. $l_n = \frac{n-1}{2}l_{n-2}$, что и тр. док.

Итак

$$l_0 = 1,\ l_2 = \frac{1}{2},\ l_4 = \frac{3}{2}l_2 = \frac{1}{2}\cdot\frac{3}{2};\ \dots\ l_{2k} = \frac{1}{2}\cdot\frac{3}{2}\cdots\frac{2k-1}{2} = \frac{2k!}{2\cdot4\cdots2k\cdot2^k} = \frac{2k!}{4^k\cdot k!}$$

$l_{2k+1} = 0$.

Лемма. Для всякого ~~действительного~~ целого числа $m \geq 1$

$$\frac{1}{\gamma}\int_{-\infty}^{\infty} e^{-\alpha^2}(y+\alpha x)^{m-1}d\alpha = \sum_{h=1}^{m}\varrho_h(y+\beta_h x)^{m-1},$$ где

$\varrho_h > 0$, и β_h действительны. (нужно доказать, что возможно соответственным выбором β_h определить ϱ_h однозначно и с знаком +).

Сравним в обеих частях коэф. при одинаковых степенях x и y:

при y^{m-1}: $\sum\varrho_h = l_0$; при $\binom{m-1}{1}y^{m-2}x$ $\sum\varrho_h\beta_h = l_1$

при $\binom{m-1}{2}y^{m-3}x^2$: $\sum\varrho_h\beta_h^2 = l_2$ и т. д.

при x^{m-1} $\sum\varrho_h\beta_h^{m-1} = l_{m-1}$.

Чтобы эти уравнения были разрешимы относ. ϱ, необх. и достаточно чтобы $\begin{vmatrix}1&1&\dots&1\\ \beta_1&\beta_2&\dots&\beta_m\\ -&-&-&-\\ \beta_1^{m-1}&\beta_2^{m-1}&\dots&\beta_m^{m-1}\end{vmatrix}\neq 0$, а это всегда будет в случае β_k действительных и различных между собою.

Пусть $\varphi(x)=a_0+a_1x+\dots+a_{m-1}x^{m-1}$ произвольный ~~функция~~ многочлен $m-1^{\text{ой}}$ степени; умножаем наши уравнения для ρ_k соответственно на $a_0, a_1, \dots a_{m-1}$ и складываем:

$$\sum \rho_k\varphi(\beta_k)=a_0l_0+a_1l_1+\dots+a_{m-1}l_{m-1}=\frac{1}{\gamma}\int_{-\infty}^{\infty}e^{-\alpha^2}\varphi(\alpha)\,d\alpha.$$

Выберем теперь для β_k значения корней уравнения $f_m=0$. Докажем, что в этом случае и для любого многочлена Φ $2m-1$ степени имеет место ~~рав~~ тождество:

$$\sum\rho_k\Phi(\beta_k)=\frac{1}{\gamma}\int_{-\infty}^{\infty}e^{-\alpha^2}\Phi(\alpha)\,d\alpha.$$

В самом деле, $\Phi(\alpha)=f_m(\alpha)\cdot g_{m-1}(\alpha)+\varphi_{m-1}(\alpha)$, значит $\Phi(\beta_k)=\varphi_{m-1}(\beta_k)$; в правой части

$$\int_{-\infty}^{+\infty}e^{-\alpha^2}f_m(\alpha)\,g_{m-1}(\alpha)\,d\alpha=0$$ по доказанному.

Значит $\int_{-\infty}^{\infty}e^{-\alpha^2}\Phi(\alpha)\,d\alpha=\int_{-\infty}^{\infty}e^{-x^2}\varphi(x)\,d\alpha$. Тождество оправдано.

Возьмем за $\Phi(\alpha)$ функцию $\left(\frac{f_m(\alpha)}{\alpha-\beta_k}\right)^2=\left((\alpha-\beta_1)\dots(\alpha-\beta_{k-1})(\alpha-\beta_{k+1})\dots(\alpha-\beta_m)\right)^2$

~~Имеем~~ Вставляем это значение в предыдущее равенство; в левой части от $\rho_1\Phi(\beta_1)+\rho_2\Phi(\beta_2)+\dots+\beta_m\Phi(\beta_m)$ останется только один член с индексом k; имеем:

$$\rho_k\Phi_k(\beta_k)=\rho_k\left(f_m'(\beta_k)\right)^2=\frac{1}{\gamma}\int_{-\infty}^{+\infty}e^{-\alpha^2}\left(\frac{f_m(\alpha)}{\alpha-\beta_k}\right)^2d\alpha,$$ т.е. ρ_k положительно. (Мы можем предположенное послед. $k=1,2,\dots m$)

Выберем теперь для β_h значения рациональные, но достаточно близкие к корням уравнения $l_m(x)=0$. ϱ_h определяются из ур-ий
$\sum\varrho_h=l_0$, $\sum\beta_h\varrho_h=l_1,\dots\sum\beta_h^{m-1}\varrho_h=l_{m-1}$, т.е. ϱ_h тоже будут рациональны. Т. к. ϱ_h суть здесь непрерывные функции β_h, то при значениях β_h достаточно близких к корням вышеупомянутого ур-ия ϱ_h останутся положительными. Итак, мы доказали тождество

$$\frac{1}{\gamma}\int_{-\infty}^{+\infty}e^{-\alpha^2}(y+\alpha x)^n d\alpha=\sum_{h=1}^{n+1}\varrho_h\left(y+\beta_h x\right)^n,$$

где ϱ_h — положит. рац. числа, β_h рациональны, кот. можно полагать $\neq 0$. Заменим $\alpha\dots\alpha_1$, $x\dots x_1$, $y\dots y+\alpha_2x_2$.

$$\frac{1}{\gamma}\int_{-\infty}^{\infty}e^{-\alpha_1^2}(y+\alpha_1x_1+\alpha_2x_2)^n d\alpha_1=\sum_{h=1}^{n+1}\varrho_h\left(y+\beta_h x_1+\alpha_2x_2\right)^n$$

Умножаем обе части на $\frac{e^{-\alpha_2^2}}{\gamma}$ и интегрируем от $-\infty$ до $+\infty$.

$$\frac{1}{\gamma}\int_{-\infty}^{+\infty}e^{-\alpha_2^2}\frac{1}{\gamma}\int_{-\infty}^{\infty}e^{-\alpha_1^2}(y+\alpha_1x_1+\alpha_2x_2)^n d\alpha_1 d\alpha_2=\frac{1}{\gamma^2}\iint_{-\infty}^{\infty}e^{-\alpha_1^2-\alpha_2^2}(y+\alpha_1x_1+\alpha_2x_2)^n d\alpha_1 d\alpha_2=$$

$$=\sum_h\varrho_h\frac{1}{\gamma}\int_{-\infty}^{+\infty}e^{-\alpha_2^2}(y+\beta_hx_1+\alpha_2x_2)^n d\alpha=\sum_{\substack{h,k\\(n+1)^2\text{ z.}}}\varrho_h\varrho_k\left(y+\beta_hx_1+\beta_kx_2\right)^n$$

Делаем замену: $y\dots y+\alpha_3x_3$, умножаем на $e^{-\alpha_3^2}\frac{1}{\gamma}$ и интегрируем по α^3 ~~от~~ $-\infty$ до $+\infty$:

$$\frac{1}{\gamma^3}\iiint_{-\infty}^{\infty}e^{-\alpha_1^2-\alpha_2^2-\alpha_3^2}(y+\alpha_1x_1+\alpha_2x_2+\alpha_3x_3)^n=\sum_{h,k,p}\varrho_h\varrho_k\varrho_p\left(y+\beta_hx_1+\beta_kx_2+\beta_px_3\right)^n \cancel{d\alpha_1 d\alpha_2}$$

и наконец:

$$\frac{1}{\gamma^5}\iiiint\!\!\int_{-\infty}^{\infty}e^{-\alpha_1^2-\alpha_2^2\dots-\alpha_5^2}(y+\alpha_1x_1+\alpha_2x_2+\dots+\alpha_5x_5)^n d\alpha_1 d\alpha_2 d\alpha_3 d\alpha_4 d\alpha_5=$$

$$=\sum_{h,k,p,q,r}\varrho_h\varrho_k\varrho_p\varrho_q\varrho_r\left(y+\beta_hx_1+\beta_kx_2+\beta_px_3+\beta_qx_4+\beta_rx_5\right)^n=$$

$$= \sum_{\lambda=1}^{N} \sigma_\lambda \left(y+\beta_{1\lambda}x_1+\beta_{2\lambda}x_2+\beta_{3\lambda}x_3+\beta_{4\lambda}x_4+\beta_{5\lambda}x_5\right)^n, \text{ где } N=(n+1)^5.$$

Итак, для данного ~~положит.~~ целого n существует целое положит. N, положительные рац. числа σ и рациональные отличные от 0 β такія, что имеет место написанное тождество.

Полагаем $y=0$; $n=2m$. Мы имѣли:

$$\frac{1}{\gamma}\int_{-\infty}^{+\infty} e^{-\alpha^2}\alpha^n\,d\alpha = 0, \text{ если } n \text{ нечетное}; \quad = \frac{2m!}{4^m\cdot m!} \text{ если } n=2m$$

Вычисляем интеграл

$$\iiiint\!\!\int_{(-\infty)}^{(+\infty)} e^{-\alpha_1^2-\alpha_2^2-\dots-\alpha_5^2}\left(\alpha_1x_1+\alpha_2x_2+\dots+\alpha_5x_5\right)^n d\alpha_1\, d\alpha_2\dots d\alpha_5.$$

Общій член подинтегральной ф-ии имеет вид:

$e^{-\alpha_1^2}\cdot\alpha_1^{n_1}\cdot e^{-\alpha_2^2}\cdot\alpha_2^{n_2}\dots e^{-\alpha_5^2}\alpha_5^{n_5}$, где $n_1+n_2+\dots+n_5=2m$; ~~т.к.~~ по предыдущему ~~члены~~ после интеграціи отличные от 0 будут получаться только от четных $n_i=2m_i$; итак $m_1+m_2+\dots+m_5=m$. ~~Интегрируем общ~~ Выполняем интеграцію в общем члене

$$\sum_{m_1+m_2+\dots+m_5=m}\frac{2m!}{2m_1!\,2m_2!\dots 2m_5!}\int_{-\infty}^{+\infty}\frac{e^{-\alpha_1^2}\alpha_1^{2m_1}}{\gamma}d\alpha_1\int_{-\infty}^{+\infty}\frac{e^{-\alpha_2^2}\alpha_2^{2m_2}}{\gamma}d\alpha_2\dots\int_{-\infty}^{+\infty}\frac{e^{-\alpha_5^2}\alpha_5^{2m_5}}{\gamma}d\alpha_5\cdot x_1^{2m_1}\dots x_5^{2m_5} =$$

$$=\sum_{m_1+m_2+\dots+m_5=m}\frac{2m!}{\cancel{2m_1!}\,\cancel{2m_2!}\dots\cancel{2m_5!}}\,x_1^{2m_1}\cdot x_2^{2m_2}\dots x_5^{2m_5}\,\frac{\cancel{2m_1}!}{4^{m_1}\cdot m_1!}\cdot\frac{\cancel{2m_2}!}{4^{m_2}m_2!}\cdots\frac{\cancel{2m_5}!}{4^{m_5}\cdot m_5!} =$$

$$=\frac{2m!}{4^m\cdot m!}\sum\frac{m!}{m_1!\,m_2!\dots m_5!}\,x_1^{2m_1}x_2^{2m_2}\dots x_5^{2m_5} = \frac{2m!}{4^m\cdot m!}\left(x_1^2+x_2^2+\dots+x_5^2\right)^m = \sum_{\lambda=1}^{N}\sigma_\lambda\left(\beta_{1\lambda}x_1+\dots+\beta_{5\lambda}x_5\right)^{2m}$$

В последней суммѣ приводим члены в скобках к общему знаменателю, ~~умножаем скобку на~~ выносим его за скобку, дѣлим обѣ части на $\frac{2m!}{4^m\cdot m!}$ и вводим новые обозначенія. Получим:

$$(x_1^2+x_2^2+\dots+x_5^2)^m=\sum_{h=1}^{N} c_h(a_{1h}x_1+a_{2h}x_2+\dots+a_{5h}x_5)^{2m},$$

где c_h — положит. рац. числа, a — целые числа $\neq 0$. Поставленное в начале теоремы тождество доказано.

Если сделаем $x_5=0$, то из этого тождества легко вывести заключение: если наша теорема справедлива для $m^{ой}$ степени, то она справедлива и для $2m^{ой}$. В с. д., обозначая общий знаменатель всех c_h через g, мы имеем: где d и a целые числа $d>0$.

$$g(x_1^2+x_2^2+x_3^2+x_4^2)^m=\sum_{h=1}^{N} d_h(a_{1h}x_1+a_{2h}x_2+a_{3h}x_3+a_{4h}x_4)^{2m};$$

По условию, каждое число = сумме конечного числа $m^{ых}$ степеней (каждое из чисел, возводимых в $m^{ую}$ степень, $=x_1^2+x_2^2+x_3^2+x_4^2$ (по теор. Lagr.)).

Пусть наше число вида gA;

$$gA=g\sum_{k=1}^{M} a_k^m = g\sum_{k=1}^{M}(x_{1k}^2+x_{2k}^2+\dots x_{4k}^2)^m=\sum g(x_{1k}^2+\dots+x_{4k}^2)^m=$$

$$=\sum_{k=1}^{M}\sum_{h=1}^{N} d_h(a_{1h}x_{1k}+a_{2h}x_{2k}+\dots+a_{4h}x_{4k})^{2m}$$; отсюда видно, что

$gA=P^{(2m)}_{S}$, где S — конечное число, не зависящее только от $2m$; Следов., любое число $B=P^{(2m)}_{S+g-1}$, что и тр. док.

2m Для доказательства теоремы в общем случае докажем следующие леммы:

Лемма 1. (Условие см. приложенный лист) Исходим из доказ. тождества

$$(x_1^2+x_2^2+\dots x_5^2)^m=\sum_{h=1}^{N} c_h(a_{1h}x_1+\dots+a_{5h}x_5)^{2m}$$

Умножая количества в скобках правой части на соответствующие целые числа, достигнем того, что на места $a_{11}, a_{12}, \dots a_{1N}$ будет стоять одно и то же число a; правая часть =

$$= \sum_{h=1}^{N} r_h \left(a x_1 + b_{1h} x_2 + \dots + b_{4h} x_5\right)^{2m},$$ где r_h полож. рац., b_{ih} — целые.

Определим A следующим образом

$$\max_{h=1,2,\dots N} \left(|b_{1h}| + |b_{2h}| + \dots + |b_{4h}|\right) + 1 = A.$$

A зависит только от данного числа m;

Заменяем x_1 через $\mathcal{G} x$; имеем:

$$\left(\mathcal{G}^2 x^2 + x_2^2 + \dots + x_5^2\right)^m = \sum_{h=1}^{N} r_h \left(a \mathcal{G} x + b_{1h} x_2 + \dots + b_{4h} x_5\right)^{2m}$$

Данное число X полагаем по форм. Лагр. $= x_2^2 + x_3^2 + x_4^2 + x_5^2$; по условию оно должно удовлетворять неравенству: $X < \Gamma^2 x^2$, т. е. $|x_2| < \Gamma x, \dots |x_5| < \Gamma x$. Затем положим:

$$X_h = b_{1h} x_2 + b_{2h} x_3 + b_{3h} x_4 + b_{4h} x_5 \gtreqless 0.$$

$|X_h| \leq |b_{1h}||x_2| + \dots + |b_{4h}||x_5| < \Gamma x \left(|b_{1h}| + \dots + |b_{4h}|\right) < A \Gamma x$, что требуется условием. Вставляя все величины, получим искомое тождество

$$\left(\mathcal{G}^2 x^2 + X\right)^m = \sum_{h=1}^{N} r_h \left(a \mathcal{G} x + X_h\right)^{2m}.$$

<u>Лемма 2.</u> (Условие см. в прил. листе). Доказ. В прошлой лемме мы имели:

$$\left(\mathcal{G}^2 x^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2\right)^m = \sum_{h=1}^{N} d_h \left(a \mathcal{G} x + b_{1h} x_2 + b_{2h} x_3 + b_{3h} x_4 + b_{4h} x_5\right)^{2m}.$$

Дифференцируем по x

$$2m \mathcal{G}^2 x \left(\mathcal{G}^2 x^2 + x_2^2 + \dots + x_5^2\right)^{m-1} = \sum_{h=1}^{N} d_h \cdot 2m \cdot a \mathcal{G} \left(a \mathcal{G} x + b_{1h} x_2 + \dots b_{4h} x_5\right)^{2m-1}.$$

Дѣлимъ обѣ части на $2m\mathcal{G}^2$ и замѣняемъ m черезъ $m+1$;
* а. α_h обозначаемъ черезъ r_h. Имѣемъ окончательно:

$$x\left(\mathcal{G}^2 x^2 + X\right)^m = \frac{1}{\mathcal{G}} \sum_{h=1}^{k'} r_h \left(a\mathcal{G}x + X_h\right)^{2m+1},$$ что и тр. док.

Лемма 3. (см. приложенный листокъ).

В качествѣ r_h выбираемъ числа, опредѣленныя в леммѣ $1^{oй}$; на основаніи этой же леммы опредѣляемъ числа a и A — цѣлыя и положительныя. Функцію $\varphi(k)$ опредѣлимъ такъ:

$$\varphi(k) = \frac{A}{\sqrt{a}}\sqrt{10k}$$ — опредѣлена для $k \geq 1$ и всегда положит.

Для опредѣленія функціи F опредѣлимъ сначала цѣлое (положительное) число $\mathcal{G}$ слѣдующимъ условіемъ:

$$(\mathcal{G}+k)^2 < K \leqq (\mathcal{G}+1+k)^2,$$

т. е. $\mathcal{G} = \mathcal{G}(K, k)$, гдѣ K — заданное цѣлое число. $\mathcal{G}$ положительно, если $1 \leqq k < \frac{1}{2}\sqrt{K} - 1$. В самомъ дѣлѣ, тогда $1+k < \sqrt{K}$, $(1+k)^2 < K$, т. е. $\mathcal{G} > 0$. Положимъ теперь

$$F(K, k) = a\mathcal{G}$$

Очевидно, $F(K, k)$ при постоянномъ k и возрастающемъ K сама возрастаетъ или остается неизмѣнной (не убываетъ); докажемъ, что она безконечно возрастаетъ вмѣстѣ с K. Для этого докажемъ неравенство:

$$k\sqrt{K} < K - \mathcal{G}^2 < 4k\sqrt{K}.$$

Изъ опредѣленія $\mathcal{G}$ мы имѣемъ: $\mathcal{G}+k < \sqrt{K} \leqq \mathcal{G}+k+1$ или

$\mathcal{G} < \sqrt{K} - k \leqq \mathcal{G}+1$, т. е. $\mathcal{G} = \sqrt{K} - k - \vartheta$, где $0 < \vartheta \leqq 1$.

~~Так. обр.~~ $\mathcal{G}$ безкон. растет вместе с K при постоянном k. Далее:

$$K - \mathcal{G}^2 = K - K + 2(k+\vartheta)\sqrt{K} - (k+\vartheta)^2 = (k+\vartheta)\left[2\sqrt{K} - (k+\vartheta)\right].$$

Отсюда

$$K - \mathcal{G}^2 < (k+1).\,2\sqrt{K} \leqq 4k\sqrt{K} ;$$

$$K - \mathcal{G}^2 \geqq (k+\vartheta)\left(2\sqrt{K} - k - 1\right) \overset{*)}{>} (k+\vartheta)\sqrt{K} > k\sqrt{K}$$

Итак, требуемыя неравенства доказаны.

Из леммы 1^ой мы имели равенство:

$$\left(\mathcal{G}^2 x^2 + X\right)^m = \sum_{h=1}^{N} r_h \left(a\mathcal{G}x + X_h\right)^{2m} ; \text{ причем } 0 < X < \Gamma^2 x^2$$
$$\text{и } |X_h| < A\Gamma x$$

Теперь за $\mathcal{G}$ (леммы 1) мы возьмем только что определенное $\mathcal{G}$

Нам надо доказать равенство:

$$\left(Kx^2 + Y\right)^m = \sum_{h=1}^{N} r_h \left(K'x + Y'_h\right)^{2m}.$$

Определим X (л. 1^ой) так: $X = (K - \mathcal{G}^2)x^2 + Y$; X-число цел. ~~положит., так.~~

Γ мы определяем так: $\Gamma = \sqrt{5k\sqrt[4]{K}}$

Докажем, что X полож. Мы имели: $K - \mathcal{G}^2 > k\sqrt{K}$; значит

$X > x^2 . k\sqrt{K} \overset{**)}{-} k\sqrt{K}x^2 = 0$. Доказано. Определим (предел) X сверху:

$X < x^2 . 4k\sqrt{K} + k\sqrt{K}.x^2 = 5k\sqrt{K}x^2 = \Gamma^2 x^2$; ~~так~~ лемма 1 приложима.

Обозначаем $a\mathcal{G} = F(K, k) = K'$; вставляем $Y'_h = X_h$.

Искомое равенство получилось; остается доказать неравенство:

---

*) Принимая во внимание: $k < \frac{1}{2}\sqrt{K} - 1$

**) На осн. неравенства $|Y| < k\sqrt{K}x^2$.

$|Y_h'| < k'\sqrt{K'}\,x$, гдѣ $k' = \varphi(k)$. Мы имѣли:
$|X_h| < A\Gamma x$ или $|Y_h'| < A\sqrt{5k}\cdot\sqrt[4]{K}\,x$ и надо показать, что это послѣднее выраженіе $< \frac{A}{\sqrt{a}}\sqrt{10k}\sqrt{a\mathcal{G}}\cdot x$ или
$A\sqrt{5k}\sqrt[4]{K}\cdot x < A\sqrt{10k}\sqrt{\mathcal{G}}\cdot x$, т. е. $\sqrt{K} < 2\mathcal{G}$;
По опредѣленію, $\sqrt{K} \leqq \mathcal{G}+k+1$; $(2k+2)^2 < K$;
$2k+2 < \sqrt{K} \leqq \mathcal{G}+k+1$; $k+1 < \mathcal{G}$. Итак $\sqrt{K} < 2\mathcal{G}$, что и тр. док.

Лемма 4. (Усл. в приложенном листкѣ).

Для N и r_h' берем соотвѣтствующія числа изъ леммы 2.
Берем основное равенство леммы 2:

$$x(\mathcal{G}^2x^2+X)^m = \frac{1}{\mathcal{G}}\sum_{h=1}^{N} r_h'(a\mathcal{G}x+X_h)^{2m+1}$$

Вводим такія же функціи φ и F, $\mathcal{G}$, Y, Y_h', Γ как в предыдущей леммѣ. получится равенство: $(a\mathcal{G} = K')$

$$x(Kx^2+Y)^m = \frac{a}{K'}\sum_{h=1}^{N} r_h'(K'x+Y_h')^{2m+1}$$, или, дѣля каждое r_h' на a и обозначая $\frac{r_h'}{a} = r_h$,

$$x(Kx^2+Y)^m = \frac{1}{K'}\sum_{h=1}^{N} r_h(K'x+Y_h')^{2m+1}$$, что и тр. док.

Лемма 5. (Условіе в отдѣльном листкѣ).

Данное число n изображаем по системѣ с основаніем 2:

$$n = 2^g + e_1\cdot 2^{g-1} + \ldots + e_g = \{1e_1\ldots e_g\}$$; здѣсь $e_h = \begin{cases}0 & \text{или}\\ 1\end{cases}$

Затѣм введем числа:

$n_0 = 1$; $n_1 = 2+e_1 = \{1e_1\}$; $n_2 = 2^2+e_1\cdot 2+e_2 = \{1e_1e_2\}$; ..... $n_g = 2^g+e_1 2^{g-1}+\ldots+e_g = \{1e_1e_2\ldots e_g\} = n$.

Из определения имеем:

$n_1 = 2n_0 + e_1$; $n_2 = 2n_1 + e_2$; ... $n_g = 2n_{g-1} + e_g$ или, вообще

$$n_{h+1} = 2n_h + e_{h+1}, \text{ где } h = 0, 1, 2, \dots g-1.$$

Каждое следующее число мы получаем, удвоив предыдущее или удвоив и прибавив затем 1.

Затем определим числа p_h:

$p_0 = \{e_1 e_2 \dots e_g\} = e_1 2^{g-1} + \dots + e_g$; $p_1 = \{e_2 \dots e_g\} = e_2 2^{g-2} + \dots + e_g$; ... ;

$p_{g-1} = \{e_g\} = e_g$; $p_g = 0$.

Между этими числами существуют соотношения:

$$p_{h-1} - p_h = e_h \cdot 2^{g-h}; \quad (h = 1, 2, \dots g); \quad p_g = 0.$$

Определим теперь p и q, входящие в условие нашей леммы.

$p = p_0 = e_1 \cdot 2^{g-1} + \dots + e_g$; $q = 2^g$; в самом деле, $p + q = \{1 e_1 \dots e_g\} = n$.

$0 \leqq p < q$. Мы утверждаем, что имеет место равенство.

$$x^{p_0}\left(K_{(0)} x^{2^g} + y_{(0)}\right)^{n_0} = \frac{1}{K'^{\,e_1}_{(0)}} \sum_{h=1}^{N} r_h^{(1)} x^{p_1} \left(K'_{(0)} x^{2^{g-1}} + y_h^{(1)}\right)^{n_1}$$

В самом деле, если $e_1 = 0$, применяем лемму 3, если $e_1 = 1$, то лемму 4. При этом полагаем:

вместо $x \dots x^{2^{g-1}}$, тогда $x^2 \dots x^{2^g}$; перенося фактор x^{p_1} вправо, имеем перед скобкой: $x^{p_0 - p_1} = x^{e_1 2^{g-1}}$. Если $e_1 = 0$, этот фактор отсутствует (случай леммы 3); если $e_1 = 1$, фактор $x^{e_1 2^{g-1}} = x^{2^{g-1}}$ соответствует x в лемме 4; в 1-м случае $n_1 = 2n_0$, во 2-м $n_1 = 2n_0 + 1$; лемма 3 или 4 всегда применима; равенство справедливо.

Докажем точно так же справедливость равенства:

$$x^{p_1}\left(K_1 x^{2^{g-1}} + Y_1\right)^{n_1} = \frac{1}{K_1'^{\,e_2}} \sum_{h=1}^{N} r_h^{(2)} x^{p_2} \left(K_1' x^{2^{g-2}} + Y_h'^{(2)}\right)^{n_2}.$$

Здесь опять 2 случая: 1) $e_2=0$, $n_2=2n_1$; тогда применяется лемма 3. $x \dots x^{2^{g-2}}$; $p_1-p_2=0$. ; 2) $e_2=1$; $n_2=2n_1+1$; $x^{p_1-p_2}=x^{2^{g-2}}$. Применим л. 4.

В обоих случаях равенство справедливо. И т. д.

Напишем предпоследнее ($(g-1)^{\text{ое}}$) равенство:

$$x^{p_{g-2}}\left(K_{g-2}x^{2^2}+Y_{g-2}\right)^{n_{g-2}} = \frac{1}{K_{g-2}'^{\,e_{g-1}}}\sum_{h=1}^{N} r_h^{(g-1)} x^{p_{g-1}} \left(K'_{g-2}x^2 + Y_h'^{(g-1)}\right)^{n_{g-1}}$$

и последнее

$$x^{p_{g-1}}\left(K_{g-1}x^2+Y_{g-1}\right)^{n_{g-1}} = \frac{1}{K_{g-1}'^{\,e_g}}\sum_{h=1}^{N} r_h^{(g)} x^0 \left(K'_{g-1}x + Y_h'^{(g)}\right)^{n_g}$$

Общий вид этого соотношения:

$$x^{p_s}\left(K_s x^{2^{g-s}} + Y_s\right)^{n_s} = \frac{1}{K_s'^{\,e_{s+1}}}\sum_{h=1}^{N} r_h^{(s+1)} x^{p_{s+1}}\left(K_s' x^{2^{g-s-1}} + Y_h'^{(s+1)}\right)^{n_{s+1}}$$

$(s=0,1,\dots,g-1).$

Каждому тождеству соответствуют числа k_s и K_s и их функции φ_s и F_s; определяем $k_s'=\varphi_s(k_s)$, $K_s'=F_s(K_s,k_s)$, определенная для $1 \leqq k_s < \frac{1}{2}\sqrt{K_s}-1$. Пусть x любое пол. число, K_s пол. число >16. Пусть Y_s дано, причем $|Y_s| < k_s K_s x^{2^{g-s}}$, тогда можно найти $Y_h'^{(s+1)}$, удовлетворяющие неравенству: $|Y_h'^{(s+1)}| < k_s'\sqrt{K_s'}\, x^{2^{g-s-1}}$.

$1^{\text{ое}}$ из чисел K (соответствующее $1^{\text{му}}$ тождеству) определим так, чтобы $|Y| < \sqrt{K}\cdot x^{g}$; последующие определим так: $K_s = K'_{s-1}$ (это возможно, т.к. в каждом новом соотношении K произвольно).

Вставляем в правую часть 1-го тождества выражения 2-го, во 2-е 3-е и т. д.; обозначим произведение $N_1 . N_2 \dots N_g = N^*$.

Мы имеем: $\left|y_h^{\prime(s+1)}\right| < k_s' \sqrt{K_s'}\, x^{2^{g-s-1}}$ и $\left|y_{s+1}\right| < k_{s+1}\sqrt{K_{s+1}}\, x^{2^{g-s-1}}$ в следующем тождестве. Т. к. $K_s' = K_{s+1}$, то, чтобы ~~отождествить~~ принять $y_h^{\prime(s+1)}$ за y_{s+1}, необходимо $k_{s+1} > k_s'$. ~~При этом~~ Итак, выбираем произвольно k_0, $K_{(0)} = K$; в частности, полагаем $k_{(0)} = 1$. Тогда определятся однозначно $k_{(0)}'$ и $K_{(0)}' = K_1$. Затем по произвольному k_1 и по K_1 определим k_1' и $K_1' = K_2$ и т. д. Наконец, по k_{g-1} (произв.) и K_{g-1} определим k_{g-1}' и K_{g-1}'. Надо еще выполнить неравенства: $k' < k_1$; $k_1' < k_2$; .... $k_{g-2}' < k_{g-1}$.

При таком выборе $\left|y_h^{\prime(s+1)}\right| < k_s'\sqrt{K_s'}\, x^{2^{g-s-1}} < k_{s+1}\sqrt{K_{s+1}}\, x^{2^{g-s-1}}$.

Итак, пусть мы выбрали K и k; ~~k_0~~ тогда

$k_0' = \varphi_0(k_0)$ полож. число. $K_1 = F_0(K, 1)$; можно при этом выбрать K так, чтобы $\frac{1}{2}\sqrt{K_1} - 1 > k' + 1$. Положим тогда $k_1 = k' + 1$. Имеем: $k_1 \geq 1$; из определения следует, что выполняются неравенства

$1 \leq k_1 < \frac{1}{2}\sqrt{K_1} - 1$.

Затем положим: $k_1' = \varphi_1(k_1)$; $K_2 = F_1(K_1, k_1)$.

Если K достаточно велико, то и K_2 настолько велико, что выполняется неравенство: $\frac{1}{2}\sqrt{K_2} - 1 > k_1' + 1$. Тогда положим $k_2 = k_1' + 1$ и так далее. Последнее определение: $k_{g-1} = k_{g-2}' + 1$ (при подходящем выборе K).

Введем обозначение: $P_h = K'_{g-1}.x + Y'^{(g)}_h$. Вставив все равенства в 1^{oe} мы получим искомое выражение:

$$x^p(Kx^q + Y) = \sum_{h=1}^{N^*} k_h P_h^n.$$

Здесь $|Y| < \sqrt{K}.x^q$; остается доказать, что все P_h положительны. Для этого надо наложить на K: должно иметь место неравенство $\sqrt{K'_{g-1}} > \kappa'_{g-1}$, где $K'_{g-1} = F_{g-1}(K_{g-1}, \kappa_{g-1})$. В самом деле, из (3) и (4)

$|Y'^{(s+1)}_h| < \kappa'_s \sqrt{K'_s}\, x^{2^{g-s-1}}$, т. е. $|Y'^{(g)}_h| < \kappa'_{g-1}\sqrt{K'_{g-1}}.x < K'_{g-1}.x$.

Поэтому $K'_{g-1}x + Y'^{(g)}_h > 0$. Лемма 5. доказана.

Переходим к доказательству самой теоремы.

Пусть дано число $n \geq 2$. Лемма 5ая утверждает существование разложения этого числа $n = p + q$; $0 \leq p < q$ и существование такого положит. целого K, что для всякого $|Y| < \sqrt{K}x^q$ им. место равенство

$$x^p(Kx^q + Y) = \sum_{h=1}^{N^*} k_h P_h^n.$$

Пусть x любое положительное целое число, $\geq 2^n$. Применим 2 раза последнюю лемму:

$$0 \leq Y_1 < \sqrt{K}x^q; \quad x^p(Kx^q - Y_1) = \sum_{h=1}^{N^*} k_h P_h^n$$

$$0 \leq Y_2 < \sqrt{K}(x+1)^q; \quad (x+1)^p(K(x+1)^q + Y_2) = \sum_{h=1}^{N^*} k_h Q_h^n$$

Складываем оба равенства.

$$x^p(Kx^q - Y_1) + (x+1)^p(K(x+1)^q + Y_2) = \sum_{h=1}^{N^*} k_h(P_h^n + Q_h^n) =$$

$$= K(x^n + (x+1)^n) + Z, \quad \text{где} \quad Z = (x+1)^p Y_2 - x^p Y_1.$$

Докажем, что каждое число Z в промежуткѣ $0 \leqq Z \leqq x^n$ может быть представлено в этом видѣ. Замѣчаем, что Діофантово уравненіе $Z=(x+1)^p \cdot Y_2 - x^p Y_1$ всегда может быть рѣшено; при этом существует одно рѣшеніе Y_2 в интервалѣ $0 \leq Y_1 < (x+1)^p$; а у нас $Y_1 < \sqrt{K}\, x^q$. Достаточно показать, что $(x+1)^p \leqq x^q$ или, т. к. $p<q$, ~~надо~~ достаточно показать, что $(x+1)^p \leqq x^{p+1}$ или $\left(1+\frac{1}{x}\right)^p \leqq x$, а это выполняется тожественно, т. к. $\left(1+\frac{1}{x}\right)^p < 2^p < 2^n \leqq x$.

Далѣе, $Y_2 = \frac{x^p Y_1 + Z}{(x+1)^p} < x^p + \frac{x^n}{x^p} = x^p + x^q \leqq x^{q-1} + x^q = x^{q-1}(1+x) < (1+x)^q$. Отсюда слѣдует, что $Y_2 < \sqrt{K}(x+1)^q$. Мы доказали наше утвержденіе.

Доказанное означает, что в видѣ суммы в правой части может быть представлено всякое число U в промежуткѣ:

$$K\left(x^n+(x+1)^n\right) \leqq U \leqq K\left(x^n+(x+1)^n\right)+x^n.$$

Начиная с нѣкотораго значенія x эти промежутки находят одни на другой; для этого необходимо:

$K\left(x^n+(x+1)^n\right)+x^n > K\left((x+1)^n+(x+2)^n\right)$, и это непремѣнно наступит при дост. большом x, т.к. слѣва коэффиціент при x^n есть $2K+1$, а справа $2K$. Итак, для $U \geqq S$ $\quad U=\sum_{h=1}^{N^*} k_h\left(P_h^n+Q_h^n\right)$

Назвав общій знаменатель всѣх k_h через E и умножая обѣ части на E, имѣем: $\quad EU = (2N^*)$ $n^{\text{ых}}$ степеней. Слѣдов., начиная с $x > ES$ каждое число мож. быть представлено в видѣ суммы ~~конечнаго~~ числа $n^{\text{ых}}$ степеней, числа, зависящаго только от n.

Теорема Waring'а доказана

Рассмотрим еще некоторые вопросы связанные с проблемой Waring'а. Мы доказали, что $N(n)$ всегда конечное число. Lagrange* доказал, что $N(2)=4$ и это действительно минимальное число, т.к. например 7 = сумме 4 квадратов. Можно поставить себе вопрос, не уменьшится ли число N, если числа рассматривать начиная с известного предела (и выше). Оказывается для $n=2$ существует бесчисленное кол. чисел, которые требуют не меньше 4^{x} квадратов — именно все числа вида $8u+7$, т.к. $z^2 \equiv 0, 4$ или $1 \pmod 8$. Назовем эту новую функцию $M(n)$; очевидно $M \leqq N$.

В случае $n=3$ $N(3)=9$, $M(3)=8$ (Landau).

Мы доказали, что $N(4) \leqq 53$, $M(4) \leqq 53$. До сих пор удалось доказать: $N(4) \leqq 37$; $N(4) \geqq 19$, т.к. $79 = 4.16 + 15.1 = 4.2^4 + 15.1^4$

Кроме того доказано, что $M(4) \geqq 16$

Приведем доказательство, что $N(4) \leqq 50$ (Realis).

Мы видели: $6y = B_{48}$; $6y+1 = B_{49}$; $6y+2 = B_{50}$

$6y+3 = 81 + 6z^{*)} = B_{49}$; $6y+4 = 16 + 6z = B_{49}$; $6y+5 = B_{50}$.

Легко показать также, что $M(4) \geqq 16$. Рассмотрим биквадратичные вычеты чисел по модулю 16. Если x четное, то $x^4 \equiv 0 \pmod{16}$; если x нечетное, то $x^2 = 8y+1$; $x^4 = 64y^2 + 16y + 1 = 16z + 1$.

$x^4 \equiv 1 \pmod{16}$.

---

*) Колошеиф. при $z = 0$, если $y \geqq 26$.

Всякое число типа $y=16u+15$ требует для своего представления по крайней мѣрѣ 15 биквадратов, $\mathcal{N}(4)\geq 15$.

Положим теперь, что число $(m\geq 1)$

$$16^m\cdot 79 = x_1^4+x_2^4+\dots+x_{15}^4.$$

Так как каждое слагаемое $\overset{\text{может быть}}{\equiv} 0$ или 1 (mod 16), а сумма $\equiv 0$ (16), то всѣ слагаемыя $\equiv 0$ (mod 16), т.е. всѣ x – четные. Полагая: $x_1=2y_1,\dots x_{15}=2y_{15}$; получим:

$$16^{m-1}\cdot 79 = y_1^4+\dots+y_{15}^4$$

; продолжая таким же образом, получили бы, что $79=B_{15}$, а это абсурд. Положение доказано (Landau).

Можно поставить задачу, аналогичную задачѣ Waring'а о разложении цѣлаго числа на сумму степеней рациональных чисел. Приведем из этой области теорему Libri:

Всякое цѣлое полож. рациональное число может быть разложено на сумму $4^х$ рациональных кубов.

Libri исходит из тождества:

$$6(x-1)^2=(2-x)^3+x^3-1-1$$

Пусть n положительное рациональное число. Определяем рац. число m так, что $\frac{n}{12}<m^3<\frac{n}{6}$ и полагаем $x=1+\frac{6m^3}{n}$. По предыдущему $\frac{1}{2}<\frac{6m^3}{n}<1$, т.е. $\frac{3}{2}<x<2$

Вставляем это выраженiе в написанное тождество:

$$6\left(\frac{6m^3}{n}\right)^2 = (2-x)^3 + x^3 - 1 - 1$$

Разрѣшаем послѣднее выраженiе относительно n.

$$n = \left(\frac{n}{6m^2}\right)^3\left((2-x)^3 + x^3 - 1 - 1\right)$$

Число n разложено т. обр. на 4 рацiональных куба, но 2 послѣдних отрицательны. Воспользуемся тождеством:

$$t-1 = t\left(1-\frac{3}{t+1}\right)^3 + \left(2-\frac{3}{t+1}\right)^3$$

; (в самом дѣлѣ, $\frac{t(t-2)^3+(2t-1)^3}{(t+1)^3} = \frac{t^4+2t^3-2t-1}{(t+1)^3} = \frac{t^4+2t^3-2t-1}{t^3+3t^2+3t+1} = t-1$).

Положим $t = x^3$; $x^3 - 1 = x^3(b-1)^3 + b^3$, гдѣ $b = 2 - \frac{3}{x^3+1}$. Тогда выраженiе $x^3 - 1 - 1 = x^3(b-1)^3 + b^3 - 1 =$ (полагаем $t = b^3$; $c = 2 - \frac{3}{b^3-1}$) $= x^3(b-1)^3 + b^3(c-1)^3 + c^3$.

Разложенiе на 4 куба достигнуто, остается показать, что $b>1$, $c>1$. ~~Докажем, что~~ Покажем, в каком случаѣ $c>1$; $1 > \frac{3}{b^3+1}$; $b^3+1>3$; $b>\sqrt[3]{2}$ — необх. условiе.

В этом случаѣ достаточно взять $x > \frac{3}{2} > \sqrt[3]{2}$; в самом дѣлѣ, тогда $2 - \frac{3}{x^3+1} > \sqrt[3]{2}$, т.к. $2 - \frac{3}{\left(\frac{3}{2}\right)^3+1} > \sqrt[3]{2}$. Теорема доказана.

В случаѣ $n=2$ легко показать: всякое рацiональное число можно представить в видѣ суммы 4х рац. квадратов. В самом дѣлѣ, $\frac{a}{b} = \frac{ab}{b^2} = \frac{Q_4}{b^2} = \sum_4$ рац. кв.

Число 4 является в то же время необходимым, например, чтобы представить число 7. Допустим, в самом дѣлѣ, что

$$7 = \left(\frac{\alpha}{\mu}\right)^2 + \left(\frac{\beta}{\mu}\right)^2 + \left(\frac{\gamma}{\mu}\right)^2, \text{ причем } (\alpha, \beta, \gamma, \mu) = 1.$$

отсюда $7\mu^2 = \alpha^2 + \beta^2 + \gamma^2$. Рассмотрим 2 случая:

1) μ нечетное; $7\mu^2 \equiv 7 \pmod 8$ и не разложимо на сумму 3 целых квадратов.

2) μ четное, левая часть четная. Из чисел α, β, γ одно только может быть четным, 2 др. нечетные. Допустив написанное равенство мы имели бы: $0 \equiv 1+1+0 \pmod 4$, абсурд. Итак, число 7 не может быть представлено в виде суммы 3 рациональных квадратов.

Конец

Оглавленіе.