Общероссийский математический портал

В. И. Арнольд, Матричная теорема Эйлера–Ферма, *Изв. РАН. Сер. матем.*, 2004, том 68, выпуск 6, 61–70

DOI: <https://doi.org/10.4213/im510>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.85.183.62

26 апреля 2023 г., 17:56:58

УДК 511

В. И. Арнольд

Матричная теорема Эйлера–Ферма

Доказаны многочисленные сравнения для биномиальных и мультиномиальных коэффициентов, а также для коэффициентов формулы Жирара–Ньютона в теории симметрических функций. Из этих сравнений вытекают также сравнения для следов различных степеней целочисленных матриц по модулю степеней простых чисел, обобщающие матричный аналог малой теоремы Ферма так же, как числовая теорема Эйлера о сравнениях обобщает числовую малую теорему Ферма.

Библиография: 4 наименования.

Теорема Эйлера, обобщающая малую теорему Ферма, $a^p \equiv a \pmod{p}$ о сравнениях по простому модулю p , имеет вид следующего сравнения по целому модулю n :

$$a^n \equiv a^{n-\varphi(n)} \pmod{n}.$$

Здесь φ – функция Эйлера, ее значение $\varphi(n)$ есть число взаимно простых с n вычетов по модулю n . Например,

$$\varphi(p) = p - 1, \quad \varphi(p^m) = (p - 1)p^{m-1},$$

так что для $n = p^m$ значение $n - \varphi(n)$ есть p^{m-1} .

В недавней статье [1] я доказал матричный аналог малой теоремы Ферма:

$$\operatorname{tr}(A^p) \equiv \operatorname{tr} A \pmod{p}.$$

В настоящей работе доказано аналогичное обобщение теоремы Эйлера для случаев $n = p^2$ и $n = p^3$:

$$\operatorname{tr}(A^{p^2}) \equiv \operatorname{tr} A^p \pmod{p^2} \quad \text{и} \quad \operatorname{tr}(A^{p^3}) \equiv \operatorname{tr} A^{p^2} \pmod{p^3},$$

где A – матрица произвольного порядка с целочисленными элементами.

Для $n = 6$, $\varphi(6) = 2$, сравнение $\operatorname{tr}(A^6) \equiv \operatorname{tr} A^2 \pmod{6}$ верно не всегда (контр-пример доставляют матрицы с собственными числами $(0, 0, \pm 1, \pm i)$).

Работа выполнена при частичной поддержке РФФИ (грант № 02-01-00655).

§ 1. Сравнения для биномиальных коэффициентов

Пусть p – простое число, a и b – неотрицательные целые числа.

ТЕОРЕМА 1. *Имеет место следующее сравнение по модулю p^2 :*

$$C_{pa}^{pb} - C_a^b \equiv 0 \pmod{p^2}.$$

ПРИМЕР. При $p = 2$ степени p , на которые делится разность из теоремы 1, образуют следующую таблицу значений показателя $x(a, b)$, определенного уравнением

$$C_{pa}^{pb} - C_a^b = p^{x(a,b)} z(a, b), \quad (p, z) = 1.$$

Для $a = 2, 3, \dots, 9$ и $0 < b < a$ числа $x(a, b)$ равны

$$\begin{array}{ccccccc} & & & & 2 & & \\ & & & & 2 & 2 & \\ & & & 3 & 6 & 3 & \\ & & 3 & 3 & 3 & 3 & \\ & 2 & 5 & 3 & 5 & 2 & \\ & 2 & 2 & 3 & 3 & 2 & 2 & \\ & 4 & 8 & 4 & 9 & 4 & 8 & 4 & \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4. \end{array}$$

При $p = 3$ аналогичная таблица значений $x(a, b)$ для $a = 2, 3, \dots, 10$ имеет вид

$$\begin{array}{ccccccc} & & & & 2 & & \\ & & & & 4 & 4 & \\ & & & 3 & 3 & 3 & \\ & & 2 & 3 & 3 & 2 & \\ & 4 & 4 & 5 & 4 & 4 & \\ & 3 & 3 & 3 & 3 & 3 & 3 & \\ & 2 & 3 & 3 & 2 & 3 & 3 & 2 & \\ & 6 & 6 & 7 & 6 & 6 & 7 & 6 & 6 & \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4. \end{array}$$

Теорема 1 утверждает, что всегда $x(a, b) \geq 2$, и я не знаю, растет ли эта функция.

Числа $x(a, b)$ обладают многими удивительными свойствами, из которых я доказал лишь немногие (ср. [2], где обсуждается и ряд гипотез).

ЛЕММА 1. *Если число c взаимно просто с p , то биномиальный коэффициент $C_{p^r a}^c$ делится на p^r .*

ДОКАЗАТЕЛЬСТВО. Воспользуемся очевидным тождеством

$$C_{p^r a}^c = \frac{p^r a}{c} C_{p^r a - 1}^{c-1}.$$

Поскольку знаменатель c взаимно прост с p , весь биномиальный коэффициент делится на p^r .

ЛЕММА 2. *Имеет место следующее сравнение по модулю p^2 :*

$$C_{pa}^{pb} \equiv C_{p(a-1)}^{p(b-1)} + C_{p(a-1)}^{pb}.$$

ДОКАЗАТЕЛЬСТВО. По определяющему треугольник Паскаля свойству биномиальных коэффициентов, число C_{pa}^{pb} равно количеству целочисленных решетчатых нестрого монотонных путей из точки $(0, 0)$ в точку (pb) строки (pa) целочисленной плоскости. Получаем рекуррентное соотношение

$$C_{pa}^{pb} = \sum_{0 \leq c \leq p} (C_{p(a-1)}^{pb-c} C_p^c)$$

(каждый путь должен в некоторой точке c пройти через уровень $\tilde{a} = p(a-1)$).

Если c отлично от 0 и p , то $(c, p) = 1$ и $(pb - c, p) = 1$, следовательно, каждый из указанных сомножителей делится на p , а их произведение делится на p^2 . По модулю p^2 вся сумма сводится к двум слагаемым с $c = 0$ и $c = p$, доставляющим сравнение леммы 2, которая, тем самым, доказана.

ЛЕММА 3. *Величины $\Delta(a, b) = C_{pa}^{pb} - C_a^b$ удовлетворяют следующим сравнениям по модулю p^2 :*

$$\Delta(a, b) \equiv \Delta(a-1, b-1) + \Delta(a-1, b).$$

ДОКАЗАТЕЛЬСТВО. Сравнение леммы 3 получается из сравнения леммы 2 вычитанием равенства

$$C_a^b = C_{a-1}^{b-1} + C_{a-1}^b.$$

Соотношение леммы 3 напоминает соотношение Паскаля, определяющее его треугольник, но является лишь сравнением.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. По модулю p^2 , числа $\Delta(a, b)$ удовлетворяют рекуррентной системе леммы 3 (определяющей и треугольник Паскаля).

Поскольку эта система уравнений однозначно определяет свое решение по начальным условиям $\Delta(a, 0)$ и $\Delta(a, a)$, остается найти эти числа:

$$\Delta(a, 0) = C_{pa}^0 - C_a^0 = 1 - 1 = 0, \quad \Delta(a, a) = C_{pa}^{pa} - C_a^a = 1 - 1 = 0.$$

Следовательно, начальные условия нулевые, а значит, и все значения $\Delta(a, b)$ нулевые (по модулю p^2), что и доказывает теорему 1.

§ 2. Сравнения для мультиномиальных коэффициентов

Мультиномиальный коэффициент разбиения натурального числа $m = \sum m_k$ на неотрицательные слагаемые m_k определяется следующим образом:

$$C(\{m_k\}) = \frac{m!}{\prod (m_k!)}.$$

Это – число слов длины m , в которых каждая буква k встречается m_k раз. Например, биномиальные коэффициенты получаются, когда слагаемых всего два:

$$C(\{m_1, m_2\}) = C_a^b,$$

где $a = m_1 + m_2$, $b = m_1$ (или $b = m_2$).

ТЕОРЕМА 2. *Имеет место следующее сравнение по модулю p^2 :*

$$C(\{pa_k\}) - C(\{a_k\}) \equiv 0 \pmod{p^2}.$$

ДОКАЗАТЕЛЬСТВО близко следует доказательству теоремы 1, приведенному выше.

ЛЕММА 4. *Если хотя бы одно из чисел a_k взаимно просто с p , а сумма $m = \sum a_k$ делится на p^r , то мультиномиальный коэффициент $C(\{a_k\})$ делится на p^r .*

ДОКАЗАТЕЛЬСТВО. Воспользуемся очевидной формулой

$$C(\{a_k\}) = \frac{m}{a_r} C(\{a_k - 1_r\}),$$

где $(p, a_r) = 1$ и где $1_r = \delta_{k,r}$ означает 1 при $k = r$ и 0 при других значениях k .

Поскольку знаменатель a_r на p не делится, мультиномиальный коэффициент, как и m , делится на p^r .

ЛЕММА 5. *Имеет место сравнение по модулю p^2 :*

$$C(\{pa_k\}) \equiv \sum_r C(\{p(a_k - 1_r)\}).$$

ДОКАЗАТЕЛЬСТВО. Мультиномиальные коэффициенты удовлетворяют рекуррентным соотношениям, аналогичным определяющему треугольник Паскаля соотношению (см., например, статью [1]):

$$C(\{pa_k\}) = \sum_c (C(\{pa_k - c_k\})C(\{c_k\})),$$

где $|c| = \sum c_k = p$ и все компоненты c_k неотрицательны.

Это свойство следует из того, что каждый (нестрого монотонный) путь b на решетке, соединяющий точки $(\{0\})$ и $(\{pa_k\})$, должен пересечь уровень $\sum b_k = p(m-1)$, где $m = \sum a_k$.

Если точка пересечения, заданная вектором c , имеет хотя бы одну взаимно простую с p координату c_k , то каждый из двух сомножителей, выписанных выше, делится на p , а их произведение делится на p^2 . Поэтому по модулю p^2 вся сумма по векторам c сводится к сумме по таким лишь векторам, у которых все компоненты делятся на p .

Поскольку, однако, $|c| = p$, такой вектор c имеет ровно одну ненулевую компоненту, скажем $c_r = p$, что и приводит всю сумму к указанному в лемме 5 виду (по модулю p^2).

ЛЕММА 6. *Величины*

$$\Delta(\{a_k\}) = C(\{pa_k\}) - C(\{a_k\})$$

удовлетворяют следующим сравнениям по модулю p^2 :

$$\Delta(\{a_k\}) \equiv \sum_r \Delta(\{a_k - 1_r\}).$$

ДОКАЗАТЕЛЬСТВО. Искомое сравнение получается вычитанием из сравнения леммы 5 равенства

$$C(\{a_k\}) = \sum_r C(\{a_k - 1_r\}).$$

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2. По модулю p^2 числа $\Delta(\{a_k\})$ удовлетворяют рекуррентной системе леммы 6 (аналогичной определению треугольника Паскаля).

Чтобы проверить единственность решения, удовлетворяющего известным нам начальным условиям

$$\Delta(\{a, 1_r\}) = C(\{pa, 1_r\}) - C(\{a, 1_r\}) = 1 - 1 = 0,$$

нужно по очереди рассматривать векторы с одной отличной от нуля компонентой (для которых мы только что доказали равенство значения Δ нулю), затем – векторы плоскости, на которой равны нулю все координаты, кроме двух.

Обращение Δ в нуль всюду на такой плоскости следует из граничных условий на двух уже исследованных прямых ввиду единственности паскалевых соотношений.

Точно так же лемма 6 позволяет доказать равенство нулю значений Δ на координатной плоскости любой размерности s , если это равенство уже известно на ее координатных гранях на единицу меньшей размерности $s - 1$.

Такой индукцией по размерности s мы приходим к выводу, что $\Delta(\{a_k\})$ сравнимо с нулем по модулю p^2 при любом разбиении $\{a_k\}$, что и доказывает теорему 2.

§ 3. Сравнения для коэффициентов формулы Жирара–Ньютона

Формула Жирара–Ньютона выражает сумму n -х степеней

$$s_n = x_1^n + \dots + x_r^n$$

через базисные симметрические функции от аргументов x_k :

$$\sigma_1 = x_1 + \dots + x_r, \quad \sigma_2 = \sum_{i < j} x_i x_j, \dots, \quad \sigma_r = \prod x_j.$$

Запишем эту формулу в виде суммы одночленов

$$s_n = \sum (K[\{m_k\}] \Pi(\{m_k\})),$$

где Π означает произведение степеней базисных функций,

$$\Pi(\{m_k\}) = \Pi(\sigma_{u_k}^{m_k}),$$

а для коэффициентов K в статье [1] доказана формула

$$K[\{m_k\}] = (-1)^{n-m} \frac{n}{m} C(\{m_k\}), \quad (*)$$

где C – мультиномиальный коэффициент, а n и m – степени полинома s_n относительно аргументов x и σ соответственно:

$$n = \sum u_k m_k, \quad m = \sum m_k.$$

Я называю описываемую формулу *формулой Жирара–Ньютона*, так как она должна была бы входить в их работы [3], [4].

ТЕОРЕМА 3. *Если $n = p$, то имеет место следующее сравнение по модулю p^2 :*

$$K[\{pm_k\}] - K[\{m_k\}] \equiv 0 \pmod{p^2}.$$

ДОКАЗАТЕЛЬСТВО. Пусть сперва p нечетно. Дробь $\frac{n}{m}$ (а также знак $(-1)^{n-m}$) не меняется при умножении степеней m_k на общий множитель p , поэтому достаточно доказать делимость на p^2 величины $\frac{n}{m} \Delta(\{m_k\})$.

Поскольку второй сомножитель, $\Delta(\{m_k\})$, делится на p^2 (теорема 2), остается проверить, что знаменатель m не может делиться на более высокую степень простого числа p , чем числитель $n = p$.

Но из формул $m = \sum m_k$, $n = \sum u_k m_k$ видно, что $m \leq n$. Поэтому m не может делиться на p^2 , так что теорема 3 выведена нами из теоремы 2, если $p \neq 2$.

В случае $p = 2$ из всех пяти возможных разбиений числа $p^2 = 4$ разбиений на четные слагаемые pm_k всего два:

$\Pi(\{m_k\})$	σ_2	σ_1^2
$K[\{m_k\}]$	-2	$+1$
$\Pi(p\{m_k\})$	σ_2^2	σ_1^4
$K[p\{m_k\}]$	$+2$	$+1$
$K[p\{m_k\}] - K[\{m_k\}]$	$+4$	0

Поскольку обе разности делятся на $p^2 = 4$, теорема 3 верна и при $p = 2$.

§ 4. Матричная теорема Эйлера

Пусть A – матрица порядка r с целочисленными элементами, tr – след, p – простое число и $n = p^2$.

ТЕОРЕМА 4. *Имеет место следующее сравнение по модулю n :*

$$\text{tr}(A^n) \equiv \text{tr}(A^{n-\varphi(n)}) \pmod{n}.$$

Здесь φ – функция Эйлера, так что для $n = p^2$ имеем $n - \varphi(n) = p$ и

$$\text{tr}(A^{p^2}) \equiv \text{tr}(A^p) \pmod{p^2}.$$

Теорема 4 эквивалентна следующей теореме теории симметричных функций.

ТЕОРЕМА 5. При $n = p^2$ имеет место сравнение

$$s_n - s_{n-\varphi(n)} \equiv 0 \pmod{n}.$$

Аналогичная матричная малая теорема Ферма, доказанная в статье [1] (где $n = p$ – простое число), утверждает вдобавок делимость на $n = p$ коэффициентов разности.

Сформулированная выше “матричная теорема Эйлера” (теорема 5) ничего не утверждает о делимости на n коэффициентов многочлена $s_n - s_{n-\varphi(n)}$: делятся на $n = p^2$ лишь значения этого целочисленного многочлена от переменных σ в каждой целой точке $\sigma \in \mathbb{Z}^r$.

ДОКАЗАТЕЛЬСТВА ТЕОРЕМ 4 И 5. Пусть p нечетно. Выражая многочлены s_n и $s_{n-\varphi(n)} = s_p$ по формуле (*) из §3, мы для получения сравнения по модулю p^2 можем пренебречь всеми слагаемыми, делящимися на p^2 .

К этому пренебрежимому классу относятся все слагаемые, для которых хотя бы один из показателей m_k взаимно прост с p . Поэтому по модулю p^2 имеет место сравнение

$$s_n - s_p \equiv \sum [K[\{pa_k\}]\Pi(\{pa_k\}) - K[\{a_k\}]\Pi(\{a_k\})].$$

Заметим теперь, что по теореме 3

$$K[\{pa_k\}] \equiv K[\{a_k\}] \pmod{p^2},$$

так что по модулю $n = p^2$ мы получили сравнение

$$s_n - s_p \equiv \sum [K[\{a_k\}](\Pi(\{pa_k\}) - \Pi(\{a_k\}))]. \quad (**)$$

Но $\Pi(\{pa_k\}) = (\Pi(\{a_k\}))^p$, поэтому разность $\Pi(\{pa_k\}) - \Pi(\{a_k\}) = \Pi^p - \Pi$ делится на p (по числовой малой теореме Ферма).

Множитель $K[\{a_k\}]$ также делится на p , так как

$$K[\{a_k\}] = (-1)^{n-m} \frac{n}{m} C(\{a_k\}),$$

причем мультиномиальный коэффициент C делится на p по лемме 4 (в самом деле, хотя бы одно из чисел a_k взаимно просто p , в противном случае число $\sum pa_k = m < n = p^2$ делилось бы на p^2), в то время как в дроби $\frac{n}{m}$ показатель p в знаменателе меньше, чем в числителе, как мы уже доказали в §3.

Итак, из сравнения (**) мы вывели сравнение

$$s_n - s_p \equiv 0 \pmod{p^2},$$

доказывающее теорему 5, а с ней и теорему 4, при нечетном p .

В случае $p = 2$ вычисления простых сравнений по модулю 4 легко провести отдельно. Рассуждая, как и выше, мы получаем сравнения

$$\begin{aligned} s_4 - s_2 &\equiv 4\sigma_4 + 4\sigma_1\sigma_3 + 2\sigma_2^2 - 4\sigma_1^2\sigma_2 + \sigma_1^4 - (-2\sigma_2 + \sigma_1^2) \\ &\equiv 2(\sigma_2^2 + \sigma_2) + (\sigma_1^4 - \sigma_1^2). \end{aligned}$$

Числа $\sigma_1^4 - \sigma_1^2$ и $2(\sigma_2^2 + \sigma_2)$ делятся на 4, что доказывает теоремы 4 и 5 и при $p = 2$.

ЗАМЕЧАНИЕ 1. Доказательство более общей матричной теоремы Эйлера,

$$\mathrm{tr}(A^n) \equiv \mathrm{tr}(A^{n-\varphi(n)}) \pmod{n}, \quad n = p^h,$$

можно, кажется, провести такими же рассуждениями, что я проверил для многих частных случаев, но не записал все детали при любом показателе h (см. также следующий § 5).

Описанных выше идей достаточно, мне кажется, чтобы установить и более сильные сравнения (например, за счет перехода от уровня pt не на p единиц вверх, как это делалось выше, а на p^2 единиц: $|c| = p^2$). На существование подобных сравнений указывают, например, таблицы примера из § 1.

§ 5. Матричная теорема Эйлера для $n = p^3$

ТЕОРЕМА 6. *Имеет место следующее сравнение по модулю $n = p^3$:*

$$\mathrm{tr}(A^n) \equiv \mathrm{tr}(A^{n-\varphi(n)}) \pmod{n}.$$

Для значения функции Эйлера φ при $n = p^3$ имеем $n - \varphi(n) = p^2$, таким образом, теорема 6 утверждает, что

$$\mathrm{tr}(A^{p^3}) \equiv \mathrm{tr}(A^{p^2}) \pmod{p^3}.$$

Этот факт эквивалентен следующей теореме теории симметрических функций.

ТЕОРЕМА 7. *Имеет место следующее сравнение по модулю $n = p^3$:*

$$s_n - s_{n-\varphi(n)} \equiv 0 \pmod{n}.$$

ЗАМЕЧАНИЕ 2. Аналогичная матричная теорема Ферма, доказанная в статье [1] (где $n = p$ – простое число), утверждает вдобавок делимость на n *коэффициентов* разности, рассматриваемой как полином от базисных симметрических функций σ_k (при $n = p$).

Матричная теорема Эйлера (теорема 7) не утверждает делимости на n *коэффициентов*: делятся на $n = p^3$ лишь *значения* этого целочисленного многочлена от переменных σ в каждой целой точке $\sigma \in \mathbb{Z}^r$.

Я не знаю, является ли эта делимость особенностью множества $\sigma(\mathbb{Z}^r)$, т. е. будут ли делиться на n значения во всех точках $\mathbb{Z}^r$ любого многочлена, значения которого во всех точках множества $\sigma(\mathbb{Z}^r)$ делятся на n .

Было бы интересно узнать, какие свойства множества $M \subset \mathbb{Z}^r$ гарантируют такую делимость всех значений многочленов, делящихся на n в точках множества M (или какие свойства специального многочлена $s_n - s_{n-\varphi(n)}$ гарантируют эту делимость).

ДОКАЗАТЕЛЬСТВА ТЕОРЕМ 6 и 7. Пусть p нечетно. Выражая многочлен s_n по формуле (*) из § 3, мы можем (для получения сравнения по модулю p^3) пренебречь всеми делящимися на p^3 слагаемыми в выражении для s_n . К этому классу относятся все слагаемые, для которых хотя бы один из показателей m_k взаимно прост с p .

Поэтому по модулю p^3 имеет место сравнение (при $n = p^3$):

$$s_n \equiv \sum [K[\{m_k\}]\Pi(\{m_k\})],$$

где все показатели m_k делятся на p .

Разобьем теперь эти слагаемые на группы в зависимости от делимости чисел $\{m_k\}$ на различные степени простого числа p : группа α содержит такие $m_k = p^\alpha a_k$, что $(a_k, p) = 1$ для некоторого k . Здесь, как и выше, $n = \sum (p^{\alpha+1} u_k a_k)$, а поделенное на p значение показателя степени мы обозначим через $\underline{n} = n/p$, $\underline{n} = p^\alpha \sum (a_k u_k)$.

Такое слагаемое вносит в $s_n - s_{n-\varphi(n)}$ вклад $I + II$, где

$$I = (K[\{p^{\alpha+1} a_k\}] - K[\{p^\alpha a_k\}])\Pi(\{p^{\alpha+1} a_k\}),$$

$$II = K[\{p^\alpha a_k\}](\pi^{p^{\alpha+1}} - \pi^{p^\alpha}),$$

и где $\pi = \Pi(\{a_k\}) = \Pi(\sigma_{u_k}^{a_k})$.

Оценим делимости обоих слагаемых I и II на степени простого числа p .

ЛЕММА 7. При $n = p^a$ слагаемое II делится на n .

ДОКАЗАТЕЛЬСТВО. Число, определенное в § 3 по формуле (*),

$$K = \pm \frac{(\underline{n} = p^{a-1})}{m} \frac{m}{(m_k = p^\alpha a_k)} C(\{m_l - 1_k\}),$$

очевидно, делится на $p^{a-\alpha-1}$. Разность $\pi^{p^{\alpha+1}} - \pi^{p^\alpha}$ делится на $p^{\alpha+1}$ (по числовой теореме Эйлера).

Итак, произведение делится на $p^{(a-\alpha-1)+(\alpha+1)} = p^a$, что и доказывает лемму 7.

Чтобы оценить вклад слагаемого I для каждого одночлена, заметим, что в числе

$$K[\{p^{\alpha+1} a_k\}] - K[\{p^\alpha a_k\}] = \frac{\underline{n}}{m} [C(\{p^{\alpha+1} a_k\}) - C(\{p^\alpha a_k\})]$$

первый множитель доставляет сомножитель $\underline{n} = p^{a-1} = p^2$, а второй сомножитель, представляющий собой мультиномиальный коэффициент, делится на p^2 по теореме 2.

Поэтому для доказательства делимости произведения на $n = p^3$ достаточно проверить, что знаменатель $m = \sum (p^\alpha a_k)$ не делится на p^2 . Случаи делимости m на p^2 легко описать, поскольку

$$(m = \sum (p^\alpha a_k)) \leq (\underline{n} = \sum (p^\alpha a_k u_k) = p^2),$$

так что делимость на p^2 числа m (которое отлично от нуля ввиду $(a_k, p) = 1$ для некоторого k) возможна только при $m = p^2$. Но из условия $m = \underline{n}$ следует,

что $p^\alpha \sum a_k = p^\alpha \sum (u_k a_k)$, так что $\sum (u_k - 1)a_k = 0$. Значит, только один коэффициент a_k отличен от нуля, для которого притом $u_k = 1$, так что $p^\alpha a_k = p^2$ и $p^{\alpha+1} a_k = p^3$. Мы заключаем, что

$$K[\{p^{\alpha+1} a_k\}] = K[\{p^\alpha a_k\}] = 1,$$

т. е. изучаемый вклад I делится на p^3 , и теорема 7 доказана для нечетных простых p .

Теоремы 6 и 7 верны и для $p = 2$ и доказываются почти так же, отличие состоит только в том, что разность

$$C(\{p^{\alpha+1} a_k\}) - C(\{p^\alpha a_k\})$$

заменяется в некоторых слагаемых (где степень m нечетна) суммой тех же мультиномиальных коэффициентов.

Эта сумма по-прежнему делится на $p^2 = 4$, что видно, например, из явной формулы для слагаемых разности $s_8 - s_4$, которых совсем не много:

$$\begin{aligned} s_8 = & \sigma_1^8 - 8\sigma_8 + 8\sigma_1\sigma_7 - 8\sigma_1^2\sigma_6 + 8\sigma_1^3\sigma_5 - 8\sigma_1^4\sigma_4 + 8\sigma_1^5\sigma_3 - 8\sigma_1^6\sigma_2 \\ & + 20\sigma_1^4\sigma_2^2 - 32\sigma_1^3\sigma_2\sigma_3 - 16\sigma_1^2\sigma_2^3 + 24\sigma_1^2\sigma_2\sigma_4 + 12\sigma_1^2\sigma_3^2 + 24\sigma_1\sigma_2^2\sigma_3 \\ & - 16\sigma_1\sigma_2\sigma_5 - 16\sigma_1\sigma_3\sigma_4 + 2\sigma_2^4 - 8\sigma_2^2\sigma_4 - 8\sigma_2\sigma_3^2 + 8\sigma_2\sigma_6 + 8\sigma_3\sigma_5 + 4\sigma_4^2. \end{aligned}$$

По модулю 8 имеет место сравнение

$$s_8 \equiv \sigma_1^8 + 20\sigma_1^4\sigma_2^2 + 12\sigma_1^2\sigma_3^2 + 2\sigma_2^4 + 4\sigma_4^2.$$

В то же время

$$s_4 = \sigma_1^4 - 4\sigma_4 + 4\sigma_1\sigma_3 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2.$$

Поэтому по модулю 8 имеет место сравнение

$$\begin{aligned} s_8 - s_4 \equiv & \sigma_1^4(\sigma_1^4 - 1) + 4\sigma_4(\sigma_4 + 1) + 2\sigma_2^2(\sigma_2^2 - 1) \\ & + 4\sigma_1^2\sigma_2(\sigma_1^2\sigma_2 + 1) + 4\sigma_1\sigma_3(3\sigma_1\sigma_3 - 1). \end{aligned}$$

Каждое из этих пяти слагаемых делится на 8, что и доказывает теоремы 6 и 7 при $p = 2$.

Список литературы

1. Арнольд В. И. Динамика Ферма, арифметика матриц, конечная окружность и конечная плоскость Лобачевского // Функцион. анализ и его прилож. 2004. Т. 38. № 1. С. 1–15.
2. Arnold Problems. Heidelberg–Berlin–N.Y.: Phasis–Springer, 2004. P. 157–162.
3. Girard A. Sur des decouvertes nouvelles en algèbre. Amsterdam, 1629.
4. Newton I. Arithmetica universalis. Cambridge, 1707.

Математический институт
им. В. А. Стеклова РАН
(119991, Москва, ул. Губкина, 8)

Поступило в редакцию
02.03.2004