Малая теорема Ферма и ее обобщения

Э. Б. Винберг

1. Три доказательства малой теоремы Ферма

Пусть p — простое число. Как известно, малая теорема Ферма утверждает, что

$$a^{p-1} \equiv 1 \pmod{p} \tag{1}$$

для всякого целого a, не делящегося на p, или, что эквивалентно,

$$a^p \equiv a \pmod{p} \tag{2}$$

для всякого целого a.

Первое доказательство. Наиболее простое, но наименее элементарное доказательство малой теоремы Ферма основано на следствии теоремы Лагранжа из теории групп, утверждающей, что порядок элемента конечной группы делит порядок группы.

Напомним, что порядком конечной группы G называется число ее элементов, а порядком элемента $g \in G$ — наименьший показатель его степени, равной единичному элементу e группы G.

Пусть G — конечная группа порядка n. Из того, что порядок элемента $g \in G$ делит n, следует, что $g^n = e$.

Рассмотрим поле $\mathbb{Z}_p$ вычетов по модулю p. Вычет целого числа a будем обозначать через $\bar{a}$. Ненулевые элементы поля $\mathbb{Z}_p$ образуют группу относительно умножения. Порядок этой группы, очевидно, равен $p-1$. Ее единичным элементом является $\bar{1}$. Следовательно, для любого целого числа a, не делящегося на p, $\bar{a}^{p-1} = \bar{1}$, но это как раз и означает сравнение (1).

Второе доказательство. (Petersen, 1872.) Пусть имеется p предметов, расположенных по кругу, каждый из которых нужно раскрасить в один из a цветов. Число всех раскрасок, очевидно, равно a^p.

Предположим, что некая раскраска переходит в себя при повороте на какой-то угол $\dfrac{2\pi d}{p}$, $0 < d < p$. Будем считать d наименьшим возможным и разделим p на d с остатком:

$$p = qd + r, \quad 0 \leqslant r < p.$$

Ясно, что данная раскраска переходит в себя при повороте на угол $\frac{2\pi qd}{p} = 2\pi - \frac{2\pi r}{p}$ и, следовательно, — и при повороте на угол $\frac{2\pi r}{p}$. В силу выбора d получаем, что $r = 0$, т. е. d делит p. Так как p — простое число, то $d = 1$, т. е. данная раскраска одноцветная.

Число одноцветных раскрасок равно a. Все остальные $a^p - a$ раскрасок разобьем на классы, отнеся к одному классу раскраски, получающиеся друг из друга поворотами. В силу предыдущего каждый класс состоит из p раскрасок. Отсюда и следует сравнение (2).

Третье доказательство. Так как при простом p все биномиальные коэффициенты C_p^k, $0 < k < p$, делятся на p (см. [1]), то в кольце $\mathbb{Z}[x, y]$ многочленов с целыми коэффициентами от переменных x и y имеет место сравнение

$$(x + y)^p \equiv x^p + y^p \pmod{p}. \tag{3}$$

(Два многочлена с целыми коэффициентами считаются сравнимыми по какому-то модулю, если их соответственные коэффициенты сравнимы по этому модулю.)

Подставляя в (3) $x = a$, $y = b$, где a, b — какие-то целые числа, мы получаем, что

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Следовательно, если $a^p \equiv a \pmod{p}$ и $b^p \equiv b \pmod{p}$, то и $(a + b)^p \equiv a+b \pmod{p}$. Так как $1^p \equiv 1 \pmod{p}$ и любое натуральное число можно получить сложением нескольких единиц, то сравнение (2) верно для всех натуральных a, а значит, и для всех целых a.

2. Теорема Эйлера

Напомним, что для любого натурального числа m через $\varphi(m)$ обозначается количество натуральных чисел, не превосходящих m и взаимно простых с m. Функция φ, называемая *функцией Эйлера*, обладает следующим свойством мультипликативности (вытекающим из китайской теоремы об остатках): если m_1 и m_2 — взаимно простые натуральные числа, то

$$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2). \tag{4}$$

Если $m = p$ — простое число, то $\varphi(m) = p - 1$; если $m = p^n$, то $\varphi(m) = p^n - p^{n-1}$.

Теорема Эйлера (сравнение Эйлера) утверждает, что

$$a^{\varphi(m)} \equiv 1 \pmod{m} \tag{5}$$

для всякого целого a, взаимно простого с m. Это, очевидно, является обобщением малой теоремы Ферма.

Если $m = m_1 m_2$, где m_1 и m_2 взаимно просты, то для доказательства сравнения (5) достаточно проверить, что

$$a^{\varphi(m)} \equiv 1 \pmod{m_1} \quad \text{и} \quad a^{\varphi(m)} \equiv 1 \pmod{m_2}. \tag{6}$$

Учитывая (4), получаем, что

$$a^{\varphi(m)} = \left(a^{\varphi(m_2)}\right)^{\varphi(m_1)} = \left(a^{\varphi(m_1)}\right)^{\varphi(m_2)}$$

и, значит, сравнения (6) вытекают из теоремы Эйлера для модулей m_1 и m_2. Это рассуждение показывает, что теорему Эйлера достаточно доказать для $m = p^n$, где p — простое число. В этом случае она принимает вид

$$a^{p^n - p^{n-1}} \equiv 1 \pmod{p^n} \tag{7}$$

для всякого целого a, не делящегося на p.

Сравнение (7) эквивалентно сравнению

$$a^{p^n} \equiv a^{p^{n-1}} \pmod{p^n}, \tag{8}$$

причем последнее сравнение, очевидно, верно и при a, кратном p, так как в этом случае обе его части делятся на p^n.

Приведем три доказательства теоремы Эйлера, обобщающие соответствующие доказательства малой теоремы Ферма.

Первое доказательство. Рассмотрим кольцо $\mathbb{Z}_m$ вычетов по модулю m. Вычет целого числа a будем обозначать через $\bar{a}$. Обратимые элементы кольца $\mathbb{Z}_m$ образуют группу относительно умножения. Как известно (и легко доказывается), элемент $\bar{a}$ обратим в $\mathbb{Z}_m$ тогда и только тогда, когда число a взаимно просто с m. Значит, порядок группы обратимых элементов равен $\varphi(m)$. Отсюда, как и в первом доказательстве малой теоремы Ферма, следует сравнение (5).

Второе доказательство. Пусть имеется p^n предметов, расположенных по кругу, каждый из которых нужно раскрасить в один из a цветов. Число всех раскрасок равно a^{p^n}. Как и во втором доказательстве малой теоремы Ферма, можно показать, что если какая-то раскраска переходит в себя при нетривиальном повороте, то она является периодической с периодом, делящим p^{n-1}. Число таких раскрасок равно $a^{p^{n-1}}$ (достаточно задать цвета каких-либо p^{n-1} расположенных подряд предметов).

Оставшиеся $a^{p^n} - a^{p^{n-1}}$ апериодических раскрасок разобьем на классы, отнеся к одному классу раскраски, получаемые друг из друга поворотами. В силу предыдущего каждый класс состоит из p^n раскрасок. Отсюда и следует сравнение (8).

Третье доказательство. Это доказательство сложнее двух предыдущих, но его идеи будут полезны нам в дальнейшем для доказательства обобщения теоремы Эйлера на алгебраические числа.

Для любого целого числа N будем обозначать через $\operatorname{ord}_p N$ показатель наибольшей степени p, на которую делится N. Докажем, что

$$\operatorname{ord}_p C_{p^n}^k = n - \operatorname{ord}_p k \text{ при } 0 < k < p^n. \tag{9}$$

Это частный случай теоремы Куммера, позволяющей найти максимальную степень p, на которую делится любой заданный биномиальный коэффициент (см. [1]), но мы дадим здесь независимое доказательство.

Имеем, прежде всего,

$$\operatorname{ord}_p C_{p^n}^1 = \operatorname{ord}_p p^n = n.$$

Далее, при увеличении k на единицу в формуле

$$C_{p^n}^k = \frac{p^n(p^n-1)\cdot\ldots\cdot(p^n-k+1)}{1\cdot 2\cdot\ldots\cdot k}$$

добавляется по одному множителю в числителе и знаменателе, причем только один из них может делиться на p. Поэтому

$$\operatorname{ord}_p C_{p^n}^{k+1} = \begin{cases} \operatorname{ord}_p C_{p^n}^k, & \text{если } k \text{ и } k+1 \text{ не делятся на } p, \\ \operatorname{ord}_p C_{p^n}^k - \ell, & \text{если } \operatorname{ord}_p(k+1) = \ell > 0, \\ \operatorname{ord}_p C_{p^n}^k + \ell, & \text{если } \operatorname{ord}_p(k) = \ell > 0. \end{cases}$$

Таким образом, при прохождении каждого числа, кратного p, $\operatorname{ord}_p C_{p^n}^k$ уменьшается, но уже на следующем шаге статус-кво восстанавливается. Отсюда и следует (9).

Группируя в формуле бинома Ньютона

$$(x+y)^{p^n} = \sum_{k=0}^{p^n} C_{p^n}^k x^{p^n-k} y^k$$

слагаемые с одинаковыми значениями $\operatorname{ord}_p k$, получаем разложение

$$(x+y)^{p^n} = x^{p^n} + y^{p^n} + \sum_{\ell=1}^{n} p^\ell f_\ell(x^{p^{n-\ell}}, y^{p^{n-\ell}}), \tag{10}$$

где $f_1, \ldots, f_n$ — какие-то многочлены с целыми коэффициентами. Это разложение является обобщением сравнения (3).

Сравнение (3) означает, что

$$(x+y)^p = x^p + y^p + ph(x,y),$$

где $h \in \mathbb{Z}[x,y]$. Возводя это равенство в степень p^{n-1} и пользуясь формулой

бинома Ньютона и равенством (9), получаем сравнение

$$(x+y)^{p^n} \equiv (x^p + y^p)^{p^{n-1}} \pmod{p^n}. \tag{11}$$

Основываясь на разложении (10) и сравнении (11), мы покажем, что если сравнение (8) выполняется для двух целых чисел a и b (для всех степеней p), то оно выполняется и для их суммы. Так как оно, очевидно, выполняется для единицы, то отсюда следует, что оно выполняется для всех целых чисел.

Итак, пусть при всех n верно, что

$$a^{p^n} \equiv a^{p^{n-1}} \pmod{p^n}, \qquad b^{p^n} \equiv b^{p^{n-1}} \pmod{p^n}.$$

Из (11) следует, что

$$(a+b)^{p^n} \equiv (a^p + b^p)^{p^{n-1}} \pmod{p^n}.$$

Записывая разложение (10) для показателя $n-1$ и подставляя $x = a^p$, $y = b^p$, получаем:

$$(a^p + b^p)^{p^{n-1}} = a^{p^n} + b^{p^n} + \sum_{\ell=1}^{n-1} p^\ell g_\ell(a^{p^{n-\ell}}, b^{p^{n-\ell}}),$$

где $g_1, \ldots, g_{n-1}$ — какие-то многочлены с целыми коэффициентами. Так как

$$a^{p^{n-\ell}} \equiv a^{p^{n-\ell-1}} \pmod{p^{n-\ell}}, \qquad b^{p^{n-\ell}} \equiv b^{p^{n-\ell-1}} \pmod{p^{n-\ell}},$$

то

$$p^\ell g_\ell(a^{p^{n-\ell}}, b^{p^{n-\ell}}) \equiv p^\ell g_\ell(a^{p^{n-1-\ell}}, b^{p^{n-1-\ell}}) \pmod{p^n}.$$

Следовательно,

$$(a+b)^{p^n} \equiv a^{p^{n-1}} + b^{p^{n-1}} + \sum_{\ell=1}^{n-1} p^\ell g_\ell(a^{p^{n-1-\ell}}, b^{p^{n-1-\ell}}) = (a+b)^{p^{n-1}} \pmod{p^n},$$

что и требовалось доказать.

Задача 1. *Докажите, что для составного m утверждение малой теоремы Ферма (т. е. сравнение $a^m \equiv a \pmod{m}$ при всех целых a) может быть верно, только если m является произведением не менее трех различных нечетных простых чисел, и что наименьшее составное m, для которого это утверждение верно — это* 561.

3. Теорема Гаусса

В случае $m = p^n$ теорема Эйлера может быть записана в форме сравнения (8). Естественно спросить, что является аналогом этого сравнения в общем случае. Ответ на этот вопрос дается теоремой Гаусса: если

$m = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ — разложение m на простые множители, то

$$a^m - \sum_{i=1}^{s} a^{\frac{m}{p_i}} + \sum_{\substack{i,j=1 \\ i<j}}^{s} a^{\frac{m}{p_i p_j}} - \cdots + (-1)^s a^{\frac{m}{p_1 \cdot \ldots \cdot p_s}} \equiv 0 \pmod{m}. \qquad (12)$$

Например, при $m = 360$ имеем:

$$a^{360} - a^{180} - a^{120} - a^{72} + a^{60} + a^{36} + a^{24} - a^{12} \equiv 0 \pmod{360}. \qquad (13)$$

Сравнение (12) было доказано Гауссом только для простых a; в общем случае оно было доказано сразу несколькими математиками в 1880-е гг. Оно является легким следствием теоремы Эйлера. Не проводя формального доказательства в общем случае, продемонстрируем его на приведенном выше примере.

Для доказательства сравнения (13) достаточно проверить, что его левая часть A делится на 8, 9 и 5. Пользуясь теоремой Эйлера для этих модулей, получаем:

$$\begin{aligned}
A &= \big((a^{45})^8 - (a^{45})^4\big) - \big((a^{15})^8 - (a^{15})^4\big) - \big((a^9)^8 - (a^9)^4\big) + \\
&\quad + \big((a^3)^8 - (a^3)^4\big) \equiv 0 \pmod{8}, \\
A &= \big((a^{40})^9 - (a^{40})^3\big) - \big((a^{20})^9 - (a^{20})^3\big) - \big((a^8)^9 - (a^8)^3\big) + \\
&\quad + \big((a^4)^9 - (a^4)^3\big) \equiv 0 \pmod{9}, \\
A &= \big((a^{72})^5 - a^{72}\big) - \big((a^{36})^5 - a^{36}\big) - \big((a^{24})^5 - a^{24}\big) + \\
&\quad + \big((a^{12})^5 - a^{12}\big) \equiv 0 \pmod{5}.
\end{aligned}$$

Задача 2. *Докажите, что если a не делится на 2 и 5, то десятичная запись числа $a^{90} - a^{40} - a^{10}$ оканчивается на 99.*

4. Малая теорема Ферма для алгебраических чисел

Многочлен от одной переменной называется *нормированным*, если его старший коэффициент равен единице. Корни многочленов с целыми коэффициентами называются *алгебраическими числами*, а корни нормированных многочленов с целыми коэффициентами — *целыми алгебраическими числами*.

Пусть $a_1, \ldots, a_d$ — (вообще говоря, комплексные) корни нормированного многочлена $f \in \mathbb{Z}[x]$ степени d. Из формул Виета следует, что элементарные симметрические функции от $a_1, \ldots, a_d$ с точностью до знака равны коэффициентам многочлена f и, стало быть, являются обычными целыми числами. Более того, пусть $F \in \mathbb{Z}[x_1, \ldots, x_d]$ — произвольный симметрический многочлен с целыми коэффициентами; тогда по основной теореме о симметрических многочленах F представляется в виде многочлена

с целыми коэффициентами от элементарных симметрических функций и, следовательно, $F(a_1, \ldots, a_d) \in \mathbb{Z}$.

Следующая теорема является обобщением малой теоремы Ферма на алгебраические числа.

Теорема 1 (T. Schönemann, 1839). *Пусть $a_1, \ldots, a_d$ — корни нормированного многочлена $f \in \mathbb{Z}[x]$ степени d и p — простое число. Тогда*

$$a_1^p + \cdots + a_d^p \equiv a_1 + \cdots + a_d \pmod{p}. \tag{14}$$

Доказательство. Индукцией по числу переменных, исходя из сравнения (3), легко получить сравнение

$$(x_1 + \cdots + x_d)^p \equiv x_1^p + \cdots + x_d^p \pmod{p} \tag{15}$$

в кольце $\mathbb{Z}[x_1, \ldots, x_d]$. Подставляя в (15) $x_1 = a_1, \ldots, x_d = a_d$ и используя малую теорему Ферма в обычном варианте, получаем

$$a_1^p + \cdots + a_d^p \equiv (a_1 + \cdots + a_d)^p \equiv a_1 + \cdots + a_d \pmod{p},$$

что и требовалось доказать.

В качестве примера рассмотрим квадратный трехчлен $f = x^2 - 2x - 1$. Его корни — это $a_1 = 1 + \sqrt{2}$, $a_2 = 1 - \sqrt{2}$. При $p = 5$ получаем

$$a_1^5 + a_2^5 = 2(1 + 10 \cdot 5 + 5 \cdot 25) = 352 \equiv 2 = a_1 + a_2 \pmod{5}.$$

(Члены, содержащие $\sqrt{2}$, сокращаются.)

Следствие. *В обозначениях теоремы* 1, *если $F \in \mathbb{Z}[x_1, \ldots, x_d]$ — любой симметрический многочлен, то*

$$F(a_1^p, \ldots, a_d^p) \equiv F(a_1, \ldots, a_d) \pmod{p}. \tag{16}$$

Доказательство. Обозначим через $S(x_1^{k_1} \ldots x_d^{k_d})$ сумму всех различных одночленов, получаемых из $x_1^{k_1} \ldots x_d^{k_d}$ перестановками переменных. Например, при $d = 4$

$$S(x_1^2 x_2 x_3) = x_1^2(x_2x_3 + x_2x_4 + x_3x_4) + x_2^2(x_1x_3 + x_1x_4 + x_3x_4) + \\ + x_3^2(x_1x_2 + x_1x_4 + x_2x_4) + x_4^2(x_1x_2 + x_1x_3 + x_2x_3).$$

Ясно, что всякий симметрический многочлен с целыми коэффициентами является целочисленной линейной комбинацией многочленов такого вида. Поэтому достаточно доказать сравнение (16) в случае, когда $F = S(x_1^{k_1} \ldots x_d^{k_d})$.

Итак, пусть $F = S(x_1^{k_1} \ldots x_d^{k_d})$. Обозначим через $y_1, \ldots, y_\ell$ члены многочлена F и через $b_1, \ldots, b_\ell$ — их значения при $x_1 = a_1, \ldots, x_d = a_d$. Ясно, что

элементарные симметрические функции от $y_1, \dots, y_\ell$ — это какие-то симметрические многочлены с целыми коэффициентами от $x_1, \dots, x_d$. Следовательно, элементарные симметрические функции от $b_1, \dots, b_\ell$ являются целыми числами, а это означает, что $b_1, \dots, b_\ell$ суть корни некоторого нормированного многочлена с целыми коэффициентами. По теореме 1

$$b_1^p + \dots + b_\ell^p \equiv b_1 + \dots + b_\ell \pmod{p},$$

но это и есть сравнение (16).

5. Теорема Эйлера для алгебраических чисел

Обобщением теоремы Эйлера на алгебраические числа является

Теорема 2 (C. J. Smyth [2], 1986). *В обозначениях теоремы* 1,

$$a_1^{p^n} + \dots + a_d^{p^n} \equiv a_1^{p^{n-1}} + \dots + a_d^{p^{n-1}} \pmod{p^n}. \tag{17}$$

Следствие. *Если* $F \in \mathbb{Z}[x_1, \dots, x_d]$ *— любой симметрический многочлен, то*

$$F(a_1^{p^n}, \dots, a_d^{p^n}) \equiv F(a_1^{p^{n-1}}, \dots, a_d^{p^{n-1}}) \pmod{p}. \tag{18}$$

Вывод этого следствия дословно повторяет вывод следствия теоремы 1. Для дальнейшего нам важно отметить, что это рассуждение показывает, что если утверждение теоремы 2 верно для каких-то фиксированных p и n (но для всех целочисленных многочленов f), то утверждение следствия верно для тех же p и n.

Доказательство теоремы 2, данное в [2], основано на формулах Ньютона, выражающих рекуррентным образом степенные суммы через элементарные симметрические функции, и довольно хитрой комбинаторной интерпретации степенных сумм корней нормированного целочисленного многочлена в духе приведенного выше второго доказательства теоремы Эйлера. Мы дадим другое доказательство, основанное на идеях приведенного выше третьего доказательства теоремы Эйлера.

Получим вначале следующее обобщение разложения (10) на произвольное число переменных:

$$(x_1 + \dots + x_d)^{p^n} = x_1^{p^n} + \dots + x_d^{p^n} + \sum_{\ell=1}^{n} p^\ell f_\ell(x_1^{p^{n-\ell}}, \dots, x_d^{p^{n-\ell}}), \tag{19}$$

где $f_1, \dots, f_n$ — какие-то многочлены с целыми коэффициентами. Иными словами, докажем, что если не все показатели $k_1, \dots, k_d$ какого-то члена $cx_1^{k_1} \dots x_d^{k_d}$ многочлена $(x_1 + \dots + x_d)^{p^n}$ делятся на $p^{n-\ell}$, то коэффициент c делится на $p^{\ell+1}$. Пусть для определенности k_1 не делится на $p^{n-\ell}$. Тогда, полагая в формуле (10) $x = x_1$, $y = x_2 + \dots + x_d$, мы получаем требуемое.

Можно считать, что f_ℓ не содержит членов, все показатели которых делятся на p: иначе соответствующий член многочлена $p^\ell f_\ell(x_1^{p^{n-\ell}}, \ldots, x_d^{p^{n-\ell}})$ можно было бы отнести к предыдущему слагаемому разложения (19). При этом условии многочлены $f_1, \ldots, f_n$ определены однозначно и, следовательно, являются симметрическими (поскольку симметрическим является многочлен $(x_1 + \cdots + x_d)^{p^n}$).

Так же, как из сравнения (3) следует сравнение (11), из сравнения (15) следует сравнение

$$(x_1 + \cdots + x_d)^{p^n} \equiv (x_1^p + \cdots + x_d^p)^{p^{n-1}} \pmod{p^n}. \tag{20}$$

Запишем разложение (19) для показателя $n-1$:

$$(x_1 + \cdots + x_d)^{p^{n-1}} = x_1^{p^{n-1}} + \cdots + x_d^{p^{n-1}} + \sum_{\ell=1}^{n-1} p^\ell g_\ell(x_1^{p^{n-1-\ell}}, \ldots, x_d^{p^{n-1-\ell}}). \tag{21}$$

Здесь $g_1, \ldots, g_{n-1}$ — какие-то многочлены с целыми коэффициентами, которые, как было сказано выше, можно считать симметрическими. Используя это разложение для правой части сравнения (20), получаем:

$$(x_1 + \cdots + x_d)^{p^n} = x_1^{p^n} + \cdots + x_d^{p^n} + \sum_{\ell=1}^{n-1} p^\ell g_\ell(x_1^{p^{n-\ell}}, \ldots, x_d^{p^{n-\ell}}). \tag{22}$$

Доказательство теоремы 2. Будем доказывать теорему индукцией по n. При $n = 1$ это теорема 1. При $n > 1$ подставим $x_1 = a_1$, …, $x_d = a_d$ в (21) и (22). По обычной теореме Эйлера

$$(a_1 + \cdots + a_d)^{p^n} \equiv (a_1 + \cdots + a_d)^{p^{n-1}} \pmod{p^n}.$$

По предположению индукции

$$g_\ell(a_1^{p^{n-\ell}}, \ldots, a_d^{p^{n-\ell}}) \equiv g_\ell(a_1^{p^{n-1-\ell}}, \ldots, a_d^{p^{n-1-\ell}}) \pmod{p^{n-\ell}}$$

при $\ell = 1, \ldots, n-1$. Следовательно,

$$a_1^{p^n} + \cdots + a_d^{p^n} \equiv a_1^{p^{n-1}} + \cdots + a_d^{p^{n-1}} \pmod{p^n},$$

что и требовалось доказать.

6. Дальнейшие следствия и обобщения

Точно так же, как из обычной теоремы Эйлера выводится сравнение (12), из теоремы 2 выводится сравнение

$$a_1^m + \cdots + a_d^m - \sum_{i=1}^{s} \left(a_1^{\frac{m}{p_i}} + \cdots + a_d^{\frac{m}{p_i}} \right) + \sum_{\substack{i,j=1 \\ i<j}}^{s} \left(a_1^{\frac{m}{p_i p_j}} + \cdots + a_d^{\frac{m}{p_i p_j}} \right) - \cdots +$$

$$+(-1)^s\left(a_1^{\frac{m}{p_1\cdot\ldots\cdot p_s}}+\cdots+a_d^{\frac{m}{p_1\cdot\ldots\cdot p_s}}\right)\equiv 0 \pmod m,$$

где $m=p_1^{k_1}\cdot\ldots\cdot p_s^{k_s}$ — разложение m на простые множители, а $a_1,\ldots,a_d$ те же, что в теореме 2. (На самом деле в [2] сразу доказывается именно это сравнение.)

В своем докладе в Московском математическом обществе (см. также [3]) В. И. Арнольд высказал в качестве гипотезы следующее утверждение: если A — целочисленная квадратная матрица, то

$$\operatorname{tr} A^{p^n}\equiv \operatorname{tr} A^{p^{n-1}} \pmod{p^n}.$$

Это утверждение является немедленным следствием теоремы 2. В самом деле,

$$\operatorname{tr} A^m=a_1^m+\cdots+a_d^m,$$

где $a_1,\ldots,a_d$ — корни характеристического многочлена матрицы A, но последний ввиду целочисленности матрицы A является нормированным многочленом с целыми коэффициентами. Можно также заметить, что гипотеза Арнольда на самом деле эквивалентна теореме 2, так как всякий нормированный многочлен с целыми коэффициентами является характеристическим многочленом некоторой целочисленной матрицы.

А. В. Зарелуа [4] доказал следующее обобщение теоремы 2. Пусть K — некоторое поле алгебраических чисел; A — кольцо его целых чисел и $\mathfrak{p}$ — простой идеал кольца A, содержащий простое число $p\in\mathbb{Z}$ и обладающий свойством

$$a^{p^n}\equiv a^{p^{n-1}} \pmod{\mathfrak{p}^n}$$

для любого $a\in A$ и любого натурального n. Пусть, далее, $a_1,\ldots,a_d$ — корни нормированного многочлена степени d с коэффициентами из A. Тогда

$$a_1^{p^n}+\cdots+a_d^{p^n}\equiv a_1^{p^{n-1}}+\cdots+a_d^{p^{n-1}} \pmod{\mathfrak{p}^n}.$$

Эта теорема может быть доказана дословным повторением приведенного выше доказательства теоремы 2 с заменой сравнений по модулю p^n сравнениями по модулю $\mathfrak{p}^n$ (хотя в работе [4] дано другое доказательство).

Список литературы

[1] Винберг Э. Б. *Удивительные арифметические свойства биномиальных коэффициентов* // Математическое просвещение. Третья серия. Вып. 12. 2008.

[2] Smyth C. J. *A coloring proof of a generalization of Fermat's little theorem* // Amer. Math. Monthly. 1986, 93, no. 6, 469–471.

[3] Arnold V. I. *On the matricial version of Fermat – Euler congruences* // Japanese J. Math. Ser. 3, 2006, 1, 1–24.

[4] Зарелуа А. В. *О матричных аналогах малой теоремы Ферма* // Матем. заметки, 2006, 79, вып. 6, 838–853.

[5] Vinberg E. B. *On some number-theoretic conjectures of V. Arnold* // Japan. J. Math., 2007, 2, 297-302.

Э. Б. Винберг, механико-математический факультет МГУ